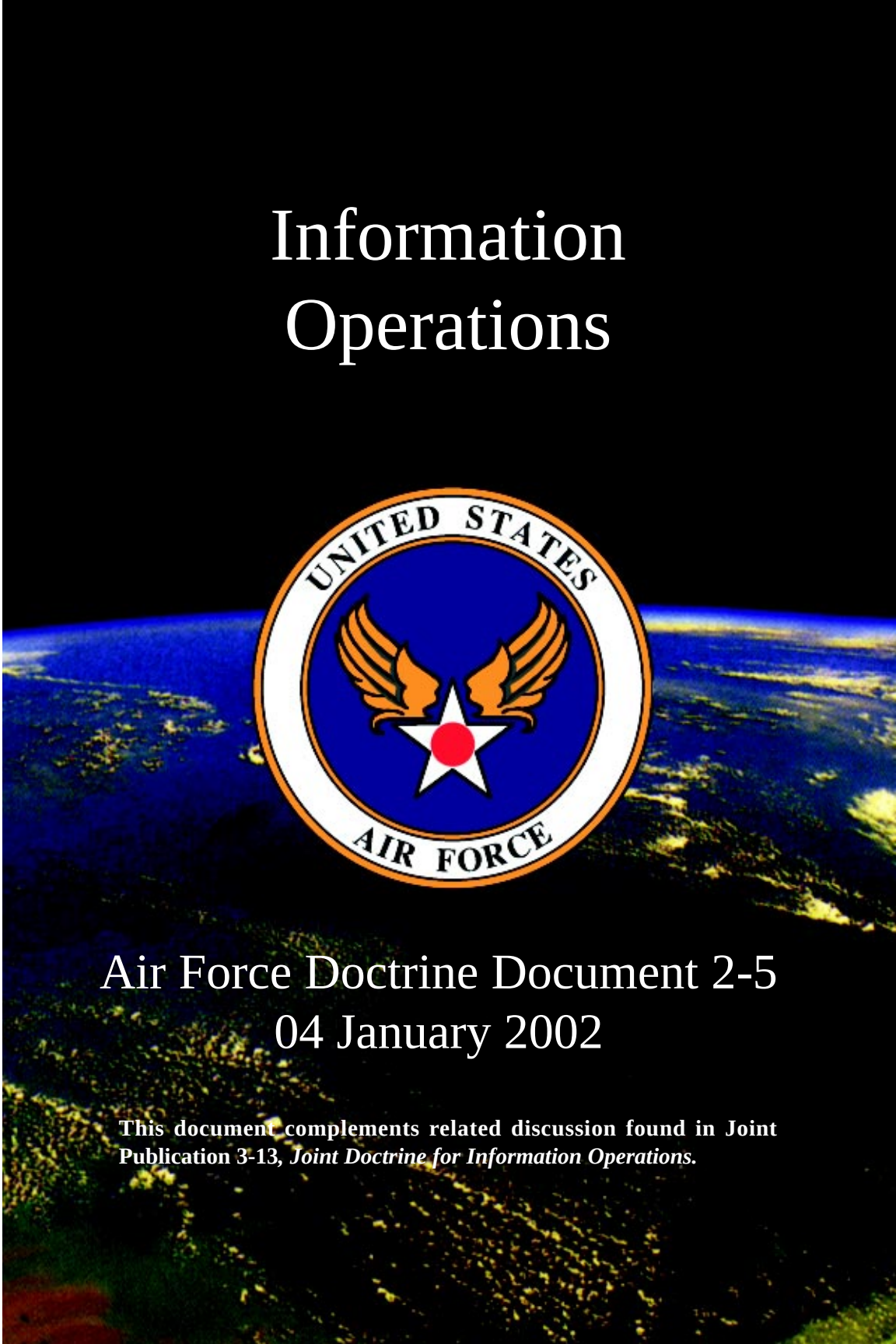
Information Operations



Air Force Doctrine Document 2-5
04 January 2002

This document complements related discussion found in Joint Publication 3-13, *Joint Doctrine for Information Operations.*

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
04/01/2002	N/A	-

Title and Subtitle Information Operations Air Force Doctrine Document 2-5	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Washington, DC	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes This document compliments Joint Pub 3-13	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** SAR
Number of Pages 80	

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE DOCTRINE DOCUMENT 2-5
04 JANUARY 2002

SUMMARY OF REVISIONS

This change revises Air Force information operations doctrine by updating key information operations concepts and terms throughout the publication, clarifies the discussion of air, space, and information superiority (Foreward and pages 1-5), and clarifies the discussion on air, space, and information warfare and counterinformation concepts (pages 11-12). This revision incorporates a discussion of information services (where appropriate and specifically in Chapter Four), establishes a separate chapter for information-in-warfare functions (Chapter Three), updates the discussion of psychological operations (pages 12-14) and information attack (to reflect use of the term computer network attack) (pages 18-19), and clarifies distinctions between information assurance and computer network defense (pages 22-24). This revision improves the discussion on electronic warfare and how it supports air, space, and information operations (pages 14-15). It introduces narrative on public affairs operations (pages 14, 17, 19-20, 26-29, and 36-38), counterpropaganda (pages 26-28), and weather operations (page 35). This revision also introduces new war-fighting organizational structures for information operations like the information warfare flight (pages 53-57); the intelligence, surveillance, and reconnaissance division (pages 51-53); and the Network Operations Security Center (Deployable) (page 57). The revision also addresses COMAFFOR-CNO responsibilities. Finally, this revision improves the discussion on information warfare targeting within the context of the overall targeting process (pages 49-50 and 56-57).

Supersedes: AFDD 2-5, 5 August 1998
OPR: HQ AFDC/DR (Maj Fredrick L. Baier and Maj Nancy Rower)
Certified by: AFDC/CC (Maj Gen David F. MacGhee, Jr.)
Pages: 78
Distribution: F
Approved by: JOHN P. JUMPER, General, USAF
Chief of Staff

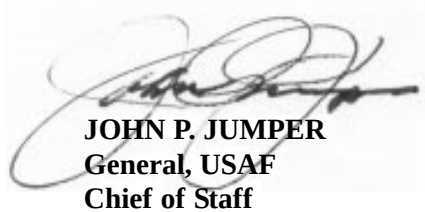
FOREWORD

Information has long been a key part of human competition—those with a superior ability to gather, understand, control, and use information have always had a substantial advantage on the battlefield. From the earliest recorded battles, to more recent military operations, history is full of examples of how the right information at the right time has influenced military struggles. The Air Force recognizes the importance of gaining a superior information advantage—an advantage obtained through information operations (IO). Information operations are those operations that achieve and maintain **information superiority**—a critical part of air and space superiority. The Air Force defines information superiority as **that degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.** Today, gaining and maintaining information superiority are critical tasks for commanders and vital elements of a fully integrated kinetic and nonkinetic effects-based operation.

Information operations are conducted across the range of military operations, from peace to war. To achieve information superiority, our understanding and practice of information operations include two distinct, but interrelated, sets of information functions: information-in-warfare and information warfare. **Information-in-warfare includes the "gain" and "exploit" information functions of IO. Information warfare, on the other hand, includes "attack" and "defend" functions.** It is also important for airmen to understand that Air Force **information services—the Air Force's piece of the global information grid that helps create and sustain the information operations medium—** underpins our ability to conduct both information-in-warfare and information warfare.

Air Force doctrine recognizes a fully integrated spectrum of military operations. Information operations, like air and space operations is effects-based. Both air and space operations can support and leverage information operations, just as information operations can support both air and space operations. Through the horizontal integration of manned, unmanned, and space assets we will enable the machine-level digital conversations that result in actionable, exploitable information for our commanders. Only in this way will airmen be able to provide the full potential of air and space power to the joint force.

Information is both a critical capability and vulnerability across the spectrum of military operations. We are prepared to achieve information superiority across that same spectrum. The United States is not alone in recognizing this need—potential adversaries worldwide are rapidly improving or pursuing their own information operations capabilities. **As the Air Force evolves into the air and space force of the twenty-first century, we will establish information capabilities and the doctrine to use them to meet the emerging challenges of the Information Age.**



JOHN P. JUMPER
General, USAF
Chief of Staff

04 January 2002

TABLE OF CONTENTS

INTRODUCTION

PURPOSE

This Air Force Doctrine Document (AFDD) explains the Air Force's war-fighting perspective on achieving information superiority through information operations. This AFDD also introduces the concept of information services, a critical requirement for air and space operations. More detailed doctrinal discussions of specific IO functions are explained in AFDD 2-5.1, *Electronic Warfare Operations*; AFDD 2-5.2, *Intelligence, Surveillance, and Reconnaissance Operations*; AFDD 2-5.3, *Psychological Operations*; and AFDD 2-5.4, *Public Affairs Operations*. Other AFDDs also discuss information operations as it applies to those specific air and space power functions.

APPLICATION

This AFDD applies to the total force: all active duty, Air Force Reserve Command, Air National Guard, and civilian Air Force personnel. **The doctrine in this document is authoritative but not directive; therefore, commanders need to consider doctrine's guidance in light of the particular situation they face.**

SCOPE

The Air Force carries out appropriate information operations actions and functions to support national and military objectives. **The term "information operations" applies across the range of military operations from peace to war.** Even when the United States is at peace, the Air Force is fully engaged, on a daily basis, in conducting some IO functions. Situational awareness, as an example, is a continuing requirement. Because of the increasing dependence on information systems and information infrastructures, the Air Force may be vulnerable to adversarial IO. Therefore, the Air Force aggressively conducts defensive counterinformation on a daily basis that deters and responds appropriately to such threats. At the far end of the range of military operations, during crisis or conflict, warfighters conduct offensive counterinformation operations while simultaneously protecting friendly information and information systems.

FOUNDATIONAL DOCTRINE STATEMENTS

Foundational doctrine statements (FDS) are the basic principles and beliefs upon which AFDDs are built. Other information in the AFDDs expands on or supports theses statements.

- **Information operations is integral to all successful air and space operations.**
- **The Air Force believes that information operations comprise those actions taken to gain, exploit, defend, or attack information and information systems.**
- **The Air Force plans to fight in the information domain by blending a variety of information-related functions to achieve the appropriate effects. Integration leads to synergistic effects.**
- **Successfully executed information operations achieve information superiority.**
- **The Air Force defines information superiority as that degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.**
- **Information superiority depends upon an effects-based approach, superior battlespace awareness, well integrated planning and execution, and information operations organizations.**
- **Without information superiority, it is difficult to achieve air and space superiority. Information superiority is a key component of air and space superiority.**
- **Information Services ensures the availability, integrity, and reliability of information—a key enabler of information superiority.**

CHAPTER ONE

THE NATURE OF INFORMATION OPERATIONS (IO)

We shape our buildings; thereafter they shape us.

Winston Churchill
(On the rebuilding of the House of Commons)

GENERAL

Information superiority is a critical part of air and space superiority, which gives the commander the freedom from attack, the freedom to maneuver, and the freedom to attack. *Information superiority is a degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.* Information superiority, like air and space superiority, is an element of combat power. The ability to support the commander with a fused, all-source, and real-time presentation of the battlespace, while at the same time complicating the view of the battlespace for an adversary, is the essence of information operations. **Improving the commander's capability to observe, orient, decide, and act (OODA Loop) faster and more effectively than an adversary is a key part of the equation.** *Information operations exist to help commanders quickly determine the situation, assess and address threats and risks, offer informed courses of action, make timely and correct decisions, and shape the battlespace to their advantage.* In essence, information operations is about integrating all appropriate aspects of combat power to influence, coerce, or compel an adversary to align their actions with US and allied objectives.

The Air Force believes that dominating the information spectrum is as critical to conflict now as controlling air and space or occupying land was in the past. Information power, like airpower and space power, is viewed as an indispensable and synergistic component of air and space power. Today, the time between the collection of information and its availability continues to shrink. Possessing, exploiting, and manipulating information have always been essential parts of warfare; these actions are critical to the outcome of future conflicts. While the traditional principles of warfare still apply, information has evolved beyond its traditional role. *Today, information is itself a weapon and a target.*

Critical to understanding air, space and information operations and its purpose—to help achieve information superiority—is a common view of what the word 'information' means. It is fundamental for airmen to clearly understand the inseparable, interrelated, and complementary nature of the two meanings of the word information as defined by the Department of Defense (DOD). The first meaning defines information as "unprocessed data of every description." Examples of unprocessed data range from the electromagnetic bits and bytes moving through information systems to graphic, oral, or written expressions of the environment gathered from the world around us. The second meaning defines 'information' as the meaning we assign to the data we perceive. From the act of interpreting data comes meaning, and ultimately from meaning comes knowledge and wisdom. **Put another way, data has limited value without the underlying meaning derived from analysis and interpretation.**

In many instances the information displayed for the commander, when traced back to its origins, rests upon an assumption, an estimate, or an extrapolation of data derived from a field trial of some weapon or item of equipment. Commanders, who have seldom participated in deriving the algorithms by which the information on display before them was drawn, tend to accept the given data as reliable fact, especially when the data are presented in numerical form. These soft links in the chain of remote inputs are fatally easy to overlook.

I. B. Holley, Jr.
(On the value of data, meaning, and command decisions)

Information superiority is an Air Force core competency upon which all the other core competencies rely. While information superiority is not solely the Air Force's domain, the airman's perspective and our global experience gained from operating in the air and space continuum make airmen uniquely prepared to achieve and use information superiority.

Joint doctrine defines IO as involving actions to affect adversary information and information systems while defending one's own information and information systems. The Air Force broadens this vision of information operations. **The Air Force believes that IO comprises those actions taken to gain, exploit, defend, or attack information and information systems** in the broadcast context of those terms. These actions (gain, exploit, defend, and attack) may occur

simultaneously. **For airmen, IO includes both information-in-warfare (IIW) and information warfare (IW).** IIW relates to the gain and exploit aspects of IO and supports all air and space functions, including IW, across all phases of operations. IW relates to the attack and defend aspects of IO and also supports all air and space functions across all phases of operations. Both IW and IIW are conducted throughout all phases of an operation and across the range of military operations.

The Air Force believes that information operations, as an element of combat power, brings together many information activities and services, occupational disciplines, resources, capabilities, and assets to help achieve effects-based operations. Information operations is an 'around-the-clock' war-fighting capability that produces effects, conducted across the spectrum of conflict, every day.

It is important to realize that the 'boundaries' between IW and IIW functions are not always clearly marked and can be somewhat artificial. For example, some information operations may begin as a systematic intelligence, surveillance, and reconnaissance (ISR) effort aimed at gaining and exploiting adversary information, but quickly transition to a defensive operation. Then seconds later, without a clearly recognized change, the effort can easily become an offensive operation—all involving many integrated capabilities and a wide variety of organizations—and all accomplished by a single, properly authorized person in a matter of minutes. There are, and will continue to be, practical overlaps between information warfare activities, information-in-warfare activities, and the activities required to maintain and protect the friendly information environment. Despite the occasional difficulty of trying to categorize different IO functions, the Air Force believes that IW, IIW, and the environment created by information services are inextricably linked and are mutually supportive. *What is important for the warfighter is that these different functional areas are integrated to achieve the appropriate battlespace effects.*

IW is information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems. Information warfare includes the attack and defend functions of information operations and is primarily conducted during times of crisis or conflict. However, the defensive functions of information warfare, much like air and space defense, are conducted across the spectrum of conflict from peace to war.

For the Air Force, the air and space power function of counterinformation is information warfare. First introduced in AFDD 1, *Air Force Basic Doctrine*, **counterinformation is the concept used to capture and express the Air Force's unique IW capabilities. Counterinformation has offensive functions—offensive counterinformation (OCI) functions—and defensive functions—defensive counterinformation (DCI) functions.** Some counterinformation operations offer new ways to achieve the commander's military objectives more efficiently in terms of lives and resources than other military operations. Ultimately, counterinformation is about integrating unique offensive and defensive air, space, and information-related means to create effects in order to achieve the commander's objectives. Accordingly, commanders should focus on the strategic, operational, and tactical effects desired in any particular situation and bring to bear the right mix of all capabilities—air, space, and information—to achieve those effects.

Information-in-warfare is a term that describes a broad range of information functions that help provide commanders the means to gain and exploit information. Effective use of IIW results in situational awareness across the spectrum of conflict. *IIW functions support all air and space operations.* IIW leverages the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on its integrated ISR assets; its global navigation and positioning capabilities, weather operations, public affairs operations, and other information collection and dissemination activities.

Successful IIW and IW operations rely heavily upon a secure, interoperable, and reliable information operations environment enabled by information services (ISvs). *State-of-the-art ISvs provide the underpinnings for successful IO,* and by extension, the achievement of information superiority and the other five Air Force core competencies. Fundamentally, ISvs is designed to match required information capabilities to the mission: get the right information to the right person in the right format at the right time.

A necessary first step towards effective air, space, and information operations is for airmen to recognize that **air, space, and information functions work best in an integrated and synergistic way.** Integrating effects-based information operations functions with the other air and space power functions is a crucial part of the Air Force's operational art.

Integration among IO functions, as well as integration of IO with other air and space operations, leads to better efficiency and mutual support; it magnifies mass, shapes priority, and can better balance air and space operations. This recognition lays the conceptual foundation for integrating information operations with other air and space operations to achieve air, space, and information superiority. The Air Force has embraced these concepts to exploit adversary vulnerabilities and limit our own potential vulnerabilities.

A Conceptual View of Information Operations

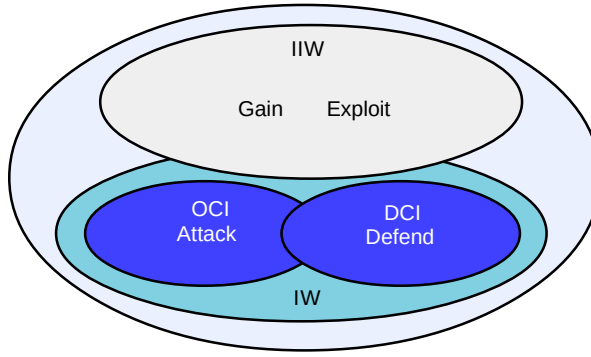


Figure 1.1. IO uses IW (attack and defend activities) and IIW function (gain and exploit activities) to help achieve information superiority.

EVOLVING INFORMATION ENVIRONMENT

Air Force IO continues to change rapidly not only in terms of technologies, but also in terms of capabilities, vulnerabilities, processes, and opportunities. One of several key features of the evolving IO environment is the exponential growth of global communications and networks. Future requirements and vulnerabilities based on the need for instant information will impact all aspects of Air Force planning.

Air Force planners must also consider our own communication requirements. This involves both the concepts and systems relating to the DOD's Global Information Grid (GIG). The GIG is important to IO and to all Air Force operations. *Airmen must have timely access to useful information to successfully achieve our objectives. The GIG facilitates this process.*

The GIG is a dynamic concept and reality. New tools such as the use of Web-based technologies, secure "chat rooms" for coordination and

information sharing, video teleconferencing for command and control, and e-mail for coordination and tasking, were recently combat-tested during Operation ALLIED FORCE. Our GIG capabilities must continue to grow to satisfy expected future demands for information, especially as our force becomes more expeditionary. By employing technology that enables the GIG to operate efficiently, we will have more accurate battlespace depictions, more decision time, a wider variety of options, and consistently more predictable effects from our weapon systems. The Air Force component of the GIG, information services (ISvs), is composed of interconnected communications and supporting information systems, including all logical and physical information assurance safeguards.

The explosion in information technologies (computers, networks, and decision tools) has already changed both the Air Force's military systems and concepts of operations in fundamental ways. The Air Force's dependence on such systems is well known and is considered both a strength and a potential vulnerability. In a world where readily available computer processing chips double their speed every 18 months, the Air Force must adapt both its technologies and its operational concepts faster than it does today. Flexibility remains, as always, the key to air and space power in the Information Age.

Another characteristic of the evolving environment is the ability of aerospace expeditionary task forces (AETFs) to reachback for products and services using the GIG. The GIG allows forward deployed personnel and organizations to obtain, process, and distribute vital intelligence, weather, and logistics information from in-theater or out of theater Service, joint, or multinational organizations. *This expanding reachback capability is vital because future AETFs will be smaller, agile, mobile, dispersed, and more reliant on reachback connectivity.* Many agencies and organizations provide reachback support through the GIG for IO or other air and space operations. Within the DOD, examples include the National Security Agency, Defense Intelligence Agency, Air Force Historical Research Agency, Joint Warfare Analysis Center, Defense Information Systems Agency, Air Force Office of Special Investigations, Secretary of the Air Force Office of Public Affairs, Air Force Communications Agency, and the Air Intelligence Agency. Outside the DOD, other organizations can provide reachback support through the GIG. Examples here include the Central Intelligence Agency and the Federal Bureau of Investigation. Reachback capabilities can yield significant advantages and should be pursued as a means of improving combat effectiveness and reducing personnel risks.

On the other hand, *commanders and leaders should also recognize emerging dependencies on reachback through the GIG and actively seek to identify and eliminate vulnerabilities through DCI operations.*

Finally, other reachback support resides in the depth and breadth of expertise and experience found within the total force. The GIG allows us to tap that experience and expertise. Subject matter experts in a variety of IO-related fields can be utilized to provide additional support to the commander's IO plans and execution.

In today's evolving environment, the Air Force's increased ability to access, process, store, and then deliver information to the warfighter, coupled with its dependence on information systems and information infrastructures, has driven the Air Force to reexamine and redefine how it integrates information-related activities into its other air and space power functions. Thus, as stated in AFDD 1, *Air Force Basic Doctrine*, dominating the information spectrum is as critical to conflict now as controlling air and space, or occupying land was in the past. Information power is viewed as an indispensable and synergistic component of air and space power.

NEW THREATS

Most information threats intend to disrupt, deny, degrade, destroy, or deceive US information or information systems. Each of the 'five D's" pose an inherent risk to both stand-alone and networked weapon and support systems. Each of the five D's is an opportunity and vulnerability—an opportunity in the sense that they offer ways in which to attack adversary systems; yet they also represent vulnerabilities that we must account for in planning our own information and information systems defenses.

The potential threats currently facing the United States are no longer defined solely by geographical or political boundaries. Potential adversaries continue to improve their IW capabilities. Advancing technology increases our society's ability to transfer information as well as an adversary's opportunity to affect that information. In some cases, new technological developments may eclipse the security designed into our current information systems. Just as the United States plans to employ IO against its adversaries, if necessary, we should expect our adversaries to have a similar capability. Numerous countries now practice both information warfare and information-in-warfare.

Examples of adversary IW techniques range from the use of psychological operations (PSYOP) to degrade or disrupt friendly operations, propaganda, electronic warfare (EW) to destroy information or deceive us, and military deception efforts. They can also use hacking cells able to attack military and key civil networks and systems on the Internet to perform any of the five D's against our information and systems. Further, state-sponsored or independent terrorists, criminal groups, and malicious hackers can be a threat to Air Force information systems. Most US socioeconomic and military infrastructures have become highly dependent on the free flow of information. *Therefore, our IO efforts should minimize any adversary's ability to impact US and friendly military information and information systems while allowing us to employ our IO strategy against our adversaries.*

In terms of IIW, some states have acquired commercially available supercomputers for a range of intelligence analysis functions; they can also access space-based imagery to help targeting efforts, secure commercial weather services, or access global positioning system (GPS) information to help increase their situational awareness and precision engagement capabilities. Adversary states can also be expected to try to use the media to their advantage and conduct intensive public affairs operations designed to shape internal and external audiences' perceptions. Furthermore, improvements in information and communication technologies allow potential adversaries to gain and share information about our vulnerabilities and capabilities.

Finally, *the range of these new threats can be described as structured or unstructured threats by looking at their organizational characteristics and purpose to determine their nature.* The structured threat is normally well organized. They usually have secure financial backing, clear objectives, and the means for infiltrating information systems to obtain information. *Structured threats include activities by state-sponsored, criminal-sponsored, or ideologically oriented groups with generally long-term objectives. Unstructured threats are generally those threats that originate from individuals or small groups with a limited support structure and limited motives; these threats are not usually sponsored by nation-states or complex organizations.* Structured and unstructured threats may be conducted by "insiders." Some "insiders" may be recruited by adversaries, while other "insiders" may pursue their own objectives. While insider acts that deliberately harm or disrupt information or information systems are not common, inadvertent

insider acts that deny service or destroy information do occur. The disruptive potential of both types of acts continues to be an area of concern.

MAIN CONSIDERATIONS

For the foreseeable future, the following are considerations for the Air Force's efforts:

- **Information superiority is a core competency upon which all other core competencies rely.**
- **Like air or space superiority, airmen must fight to achieve and maintain information superiority.**
- **The two sets of IO functions—IW and IIW—while separate and distinct, are intrinsically and inextricably linked. They must be integrated to achieve information superiority.**
- **Successful IO rests upon a secure and responsive information environment created and sustained by Air Force information services capabilities.**
- **Information operations can support, and can be supported by, all other aspects of air and space power.**
- **DCI is the Air Force's overall top priority within the information warfare arena. Commanders are accountable for DCI posture and execution within their commands.**
- **Like other air and space operations, the breadth of counterinforma-tion operations must be performed simultaneously and in parallel. Some specific counterinformation actions can alternate almost instantly between the offensive and the defensive.**
- **The Air Force performs many different information operations simultaneously at the strategic, operational, and tactical level, employing a combination of deployable and reachback capabilities, that support air and space expeditionary operations.**
- **It is important for commanders at all levels to continuously consult with their staff legal advisors when developing various information warfare courses of action.**
- **Like other air and space operations, Air Force IO should be centrally controlled and decentrally executed by airmen. IO**

should be integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide; but there should not be a separate IO plan.

- **Air Force IW efforts will focus on implementing IW capabilities in support of joint war-fighting commands.**
- **While the focus of information operations is primarily at the operational and tactical level, commanders must remain aware of the strategic consequences of any effects-based application of force. The Air Force will vigorously support national, strategic-level IO consistent with the premise that air and space power is an inherently strategic force.**
- **IO comprises several air and space power functions; IO expertise in the commander's staff should therefore be drawn from IO-trained airmen representing a broad diversity of Air Force war-fighting experience and relevant training.**

CHAPTER TWO

INFORMATION WARFARE (IW)

When blows are planned, whoever contrives them with the greatest appreciation of their consequences will have a great advantage.

Frederick the Great

Information warfare, along with information-in-warfare, is one of two subsets of information operations. **IW is focused on the attack and defend functions of information operations.** This chapter outlines the Air Force's perspective on IW.

Counterinformation is the term used to describe the Air Force's information warfare capabilities. Like the counterair or counterspace functions, the counterinformation function reflects a unique aspect of air and space power.

Counterinformation is an air and space power function which helps establish information superiority by neutralizing or influencing adversary information activities to varying degrees, depending on the situation. Joint terminology refers to this set of actions as information warfare, and in the joint environment airmen should use 'information warfare' to describe in general terms counterinformation functions. The Air Force differentiates between these two terms because in the joint arena IW is only conducted during contingencies while the Air Force believes some parts of counterinformation are conducted every day. Some counterinformation functions are conducted throughout the spectrum of conflict, as appropriate and necessary, in keeping with US policy and legal requirements. Thus, counterinformation operations can include support of military operations other than war and peacetime defense of Air Force or friendly operations. *Combined with counterair and counterspace, counterinformation creates an environment where friendly forces conduct operations with the requisite freedom of action while denying, neutralizing, or influencing adversary information activities as required.*

Counterinformation, like counterair and counterspace, consists of both offensive and defensive activities.

- **OCI and DCI parallel the traditional Air Force constructs of offensive counter (OCA) and defensive counterair (DCA).** Airmen can apply many of the hard-won precepts of OCA-DCA to OCI-DCI. As with OCA and DCA, **commanders should focus on the required effects.** The dividing line between the two can be difficult to determine and the transition nearly instantaneous.
- Offensive counterinformation includes actions taken to attack adversary information and information systems. *OCI operations are designed to limit, deny, degrade, deceive, disrupt, or destroy adversary information capabilities and are dependent on having an understanding of an adversary's information capabilities.* The term OCI is essentially synonymous with the joint term of offensive information warfare (OIW).
- **Defensive counterinformation includes those actions that protect and defend friendly information, information systems, and other information operations.** The term DCI is essentially synonymous with the joint term of defensive information warfare (DIW).

OFFENSIVE COUNTERINFORMATION (OCI) OPERATIONS

OCI functions that can affect an adversary's capabilities and exploit vulnerabilities include: PSYOP, EW, military deception, public affairs operations, computer network attack, and physical attack. All effective OCI operations always require a detailed understanding of an adversary's information capabilities, dependencies, and vulnerabilities.

Psychological Operations (PSYOP)

Focused on the human dimension of the battlespace, **PSYOP is an operational discipline that targets the mind of the adversary. In general, PSYOP seeks to induce, influence, or reinforce the perceptions, attitudes, reasoning, and behavior of foreign leaders, groups, and organizations in a manner favorable to military objectives.** PSYOP supports these objectives through the calculated use of air, space, and information power with emphasis on psychological effects-based targeting. *Operationally, it provides the air component commander an effective and versatile means of exploiting the psychological vulnerabilities of hostile forces to create fear,*

confusion, and paralysis, thus undermining their morale and fighting spirit. In this way, PSYOP prepares the battlespace (actual or potential) for successful air and space operations. As an instrument of information warfare, PSYOP leverages air and space power to help achieve a psychological balance in the battlespace that is advantageous to our forces.

COMMANDO SOLO: One example of an aerospace PSYOP tool. The principal focus of aerospace PSYOP is not platforms, but effects.

PSYOP is a key discipline within the Air Force's IO "arsenal." Used in conjunction with other IO disciplines (e.g., deception, physical attack), it can also play a central role in perception management at the strategic, operational, and tactical levels. Ideally, by manipulating—and thus "managing"—the adversary's perception of the battlespace, the combat commander can effectively control the adversary's situational awareness and decision-making process.

PSYOP is also an integral part of joint operations. Air Force PSYOP activities are extensively coordinated throughout the joint force, and in some cases, with the National Command Authorities (NCA). Thus, the Air Force neither plans nor conducts independent PSYOP campaigns. Rather, airmen contribute to the theater commander in chief's (CINC's) overall campaign objectives through the systematic use of air and space power, with a view toward shaping the battlespace psychologically.

Conversely, PSYOP activities can also help defend or safeguard military personnel and resources by preempting the hostile actions of an opposing force or leader, dissuading hostile actors from taking courses of action harmful to the interests or objectives of friendly forces, or countering the effects of hostile propaganda. *Thus, PSYOP can be employed across the range of military operations to help counter terrorist threats, protect US forces, dissuade or preempt hostile actors, and support counterpropaganda efforts.*

It is important to note that the target and thrust of any PSYOP activity (the mind of the audience) are essentially the same, regardless of whether PSYOP is used in an offensive or defensive role. Particular PSYOP activities can only be characterized as "defensive" or "offensive," after one considers both the commander's intent and the circumstances in which the activity itself is conducted.

Lastly, it is also important to remember that public affairs (PA) operations can be an offensive counterinformation tool that can work with PSYOP efforts. While PSYOP and PA operations are separate functions and quite distinct, they should be coordinated to work together with common themes towards common ends. PA operations may be used to disseminate international information, but great care must be taken to avoid any public perception that information provided through public affairs channels is slanted or manipulated.

The real target in war is the mind of the enemy commander, not the bodies of 17 of his troops.

Captain Sir Basil Liddell Hart
***Thoughts on War*, 1944**

Electronic Warfare (EW)

EW is any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack an adversary. The EW spectrum is not merely limited to radio frequencies but also includes optical and infrared regions as well. EW assists air and space forces to gain access and operate without prohibitive interference from adversary systems. During Operation DESERT STORM, effective force packaging, which included self-protection, standoff, and escort jamming and antiradiation attacks, contributed significantly to the Air Force's extremely low loss rate. More importantly, it enabled highly successful combat air operations against the Iraqi civil and military infrastructure and fielded forces.

EW is a key contributor to air superiority, space superiority, and information superiority. The most important aspect of the relationship of EW to air, space, and information operations is that *EW enhances and supports all air and space operations throughout the full spectrum of conflict and improves aerospace vehicle survivability and space system integrity.* In the near future, Air Force

EW resources and assets may take on new roles in support of air and space operations. Further, nothing in this doctrine suggests 'ownership' of EW resources and assets by specific organizations or agencies.

The three major subdivisions of EW are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). All three contribute to air and space operations, including the integrated IO effort. Control of the electromagnetic spectrum is gained by protecting friendly systems and countering adversary systems.

Electronic attack is the component involving the use of electromagnetic, directed energy (DE), or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.

Electronic warfare support (the collection of electromagnetic data for immediate tactical applications, e.g., threat avoidance, route selection, targeting, or homing) provides information required for timely tactical decisions involving electronic warfare operations.

Electronic protection (protecting personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability) enhances the use of the electronic spectrum for friendly forces. EP is also part of DCI operations.

Remember, EW is a force multiplier. Control of the electromagnetic spectrum can have a major impact on success across the range of military operations. Proper employment of EW enhances the ability of operational commanders to achieve objectives. *Electronic attack and electronic warfare support should be carefully integrated with electronic protection to be effective.* The commander should also ensure maximum coordination and deconfliction between EW, ISR, and communication activities. When EW actions are fully integrated with military operations, synergy is achieved, attrition is minimized, and effectiveness is enhanced.

Military Deception

Deception operations are a powerful tool in military operations. **Military deception misleads adversaries, causing them to act in accordance with the originator's objectives.** *Deception operations*

All warfare is based on deception.

SunTzu
***The Art of War*, 500BC**

span all levels of war and can include, at the same time, both offensive and defensive components. Deception can distract our adversaries' attention from legitimate friendly military operations and can confuse and dissipate adversary forces. However, effective deception efforts require a deep appreciation of an adversary's cultural, political, and doctrinal perceptions and decision-making processes. Planners exploit these factors for successful deception operations. Deception is another force multiplier and can enhance the effects of other information warfare activities.

Commanders should fully coordinate deception operations with other operations to insure that deception efforts are protected. There is a delicate balance between successful deception efforts and media access to ongoing operations for media coverage.

A key to well-planned and executed deception operations is anticipating adversary motives and actions. *Accurate and reliable intelligence, surveillance, and reconnaissance operations and information products* and close cooperation with counterintelligence activities help the commander anticipate adversary intentions and capabilities.

When formulating the deception concept, particular attention should be placed on defining how commanders would like the adversary to act

A classic example of military deception is World War II's Operation FORTITUDE NORTH, when the Allies heavily bombed the Pas de Calais area rather than Normandy, feeding the German bias for believing the former would be the invasion site.

A modern example of deception operations occurred during Operation DESERT STORM. US Marine Corps elements publicaly rehearsed amphibious operations and were later placed afloat just off the Kuwaiti coast to deceive Iraqi decision makers into believing an amphibious invasion of Kuwait was imminent. This deception effort fixed several Iraqi divisions in place near the Kuwaiti coast and kept them from reorienting towards approaching coalition forces until it was too late for them to effectively defend against the coalition assault.

No enterprise is more likely to succeed than one concealed from the enemy until it is ripe for execution.

Niccolo Machiavelli

at critical points. Those desired actions then become the goal of deception operations. Sufficient forces and resources should be committed to the deception effort to make it appear credible to the adversary.

Deception operations should be planned from the top down and subordinate deception plans should support higher-level plans. Plans may include the use of lower-level units, although subordinate commanders may not know of the overall deception effort. Before planning deception operations, subordinate commanders should coordinate with their senior commander to ensure overall unity of effort. *Deception efforts must not conflict with the overall joint force deception effort.* Operations security (OPSEC) may dictate only a select group of senior commanders and staff officers know which actions are purely deceptive in nature. However, commanders should carefully weigh the balance between OPSEC and detailed coordination of deception plans. Furthermore, the use of deception in the realm of IO requires particular care and coordination given the speed and potential extent of information propagation. In some cases, excessively restricting the details of planned deception operations can cause confusion at lower echelons that may negatively affect the outcome of the deception operation.

Finally, PA operations may play a part in deception planning through coordination and deconfliction. However, joint doctrine for military deception states that such operations will not intentionally target or mislead the US public, Congress, or the news media. Deception activities potentially visible to the American public should be closely integrated with PA operations so as to not compromise operational considerations nor diminish the credibility of PA operations in the national media. PA operations can document displays of force or training operations but they cannot use false information to simulate force projection. If false information were ever used in PA operations, public trust and support for the Air Force could be undermined and the capabilities provided by PA operations could be restricted from use.

Physical Attack

Physical attack disrupts, damages, or destroys adversary targets through destructive power. As an element of an integrated counterinformation effort, physical attack refers to the use of "hard kill" or *kinetic* weapons to create information effects. There are two types of effects that physical attack can provide to counterinformation efforts. First, physical attack can create a physically discernible effect against an adversary information system, for example, the destruction or disruption of a key leadership communication node. Second, physical attack can also be used to create or alter adversary perceptions. In either case, the purpose of *physical attack in a counterinformation role is to affect adversary information or information systems by using a physical weapon to create a specific effect on the adversary.*

An example of physical attack as an information operation might include the use of precision-guided munitions and advanced delivery platforms to neutralize an adversary leader's main command and control communications node. Other examples might include the use of cruise missiles or aircraft to destroy an adversary's ISR capabilities or the insertion of a special operations team to cut and/or exploit their communication lines. Further, physical attack can complement PSYOP activities. For example, well-timed physical attacks can add credibility to and intensify a previously delivered PSYOP message.

All IW physical attack operations should be integrated with other combat operations in the targeting process. IW physical attack operations should be carefully coordinated and deconflicted with other planning efforts.

Finally, standardized criteria to measure the presence, effectiveness, and duration of IW physical attack operations' effects should be developed to allow those assessments to be calculated into the overall combat assessment.

Computer Network Attack (CNA)

Computer network attacks (CNA) are operations conducted using information systems to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. The ultimate objective of

CNA is to influence the adversary commander's decisions. *Computer and telecommunication systems are the principal means to employ CNA and are primary targets of CNA operations.* This distinction is important to separate CNA activities from other IW activities such as physical attack that might target similar information systems with different means.

CNA can apply to and involve all information systems including traditional computing systems and networks as well as telecommunication systems and networks. One example of CNA includes actions taken to reduce an adversary's effectiveness by denying an adversary the unfettered use of computer or telecommunication systems by affecting the devices' ability to perform its designated mission. In another example, CNA may deceive an adversary by deleting (i.e., destroy) or distorting (i.e., degrade) information stored on, processed by, or transmitted by computer or telecommunication network devices.

Computer network attack can offer the commander the ability to incapacitate an adversary while reducing exposure of friendly forces, reducing collateral damage, or preventing excessive adversary losses. Using computer network attack capabilities and tools may save conventional sorties for other targets. *Computer network attack, like all other information operations, is most effective and efficient when integrated with other air and space operations.*

Public Affairs (PA) Operations

PA operations can also be used for offensive counterinformation operations. **PA operations can contribute to global influence and deterrence by making foreign leaders aware of US capabilities and by countering enemy propaganda with the truth.** Communicating capabilities can be a force multiplier and may deter potential adversaries by "driving a crisis back to peace" before use of force becomes necessary.

The Joint Chiefs of Staff (JCS) Joint Strategic Capabilities Plan (JSCP) recognizes that information is just as important as diplomatic, military, or economic factors by establishing **Informational Flexible Deterrent Options (IFDOs). IFDOs are options available to commanders as alternative courses of action in accomplishing operational missions other than "bombs on target"**. IFDOs heighten

public awareness; promote national and coalition policies, aims, and objectives for the operation, as well as counter adversary propaganda and disinformation in the news.

Maintaining an open dialogue with the news media communicates the leadership's concern with the issues and allows the correct information to be placed in the public sector, without media speculation or the media going to other sources (such as the adversary) for information. This heightens public awareness and helps gain and maintain public support. This increased media attention may also place enormous pressures on foreign leaders and governments and that alone may be enough to achieve the objective.

Another important task for *PA operations involves articulating US National (and/or coalition) policies, aims, and objectives.* Explaining what we intend to achieve and why it is important helps gain public understanding and support for our operations. This also helps the opponent understand what the United States and its coalition partners expect from them.

Heightening adversary awareness of the potential for conflict by keeping the issue in the news and in the headlines helps maintain national and international pressure on our opponent. This can be difficult to achieve because sometimes news media are just not interested, especially during a lull in operations. Including news media in our preparations, expanding the number of regional and hometown media involved, offering high-level spokespersons, providing strong visuals, and giving opportunities to do and see things they otherwise would not, will help gain and maintain the news media interest. These efforts take careful centralized planning and a clear understanding of what the NCA hopes to achieve by keeping issues in the news.

One way that PA operations can be used in an offensive counterinformation role is by using a virtual force projection IFDO. Conventional wisdom holds that release of information will be detrimental to military operations. However, commanders should consider the possible advantages of releasing certain information to demonstrate US resolve, intent, or preparations. Rather than providing an advantage to an adversary, the carefully coordinated release of operational information in some situations could deter military conflict.

DEFENSIVE COUNTERINFORMATION (DCI) OPERATIONS

DCI operations are those actions that protect and defend Air Force information and information systems from an adversary. Actual incidents—ranging from a teenager's computer attacks against US research and development facilities to an adversary's deliberate manipulation of systems critical to displaying the air picture for the joint force air and space component commander (JFASCC)—demonstrate how critical defending information is to military operations. Due to US dependency on and the general vulnerability of information systems, DCI is the Air Force's top priority within the information warfare arena. Accordingly, commanders are responsible for DCI posture and execution within their commands. While key elements of DCI involve protecting and defending Air Force information systems and communications networks, DCI is more than just that. The goal of DCI is to ensure the necessary protection and defense of all information and information systems that support military operations. *When combined with OCI, the net result is an enhanced opportunity to use IW functions to achieve stated military and national objectives.*

DCI functions include OPSEC, information assurance (IA), computer network defense (CND), counterdeception, counterintelligence, PA operations, counterpropaganda operations, and electronic warfare (principally electronic protection). These various defensive capabilities are mutually supporting (that is, any one can be used as a countermeasure or in support of one another) and can support offensive activities. Additionally, to capitalize on defensive information effects, the capabilities are best applied in a "layered defense" approach. However, they can at times also conflict with each other and with offensive activities if they are not coordinated ahead of time. For example, CND activities might work to minimize an information system's security breach as quickly as possible to defend the systems, while counterintelligence activities might want to allow continued access to identify and exploit the adversary.

Operations Security (OPSEC)

OPSEC is a DCI function that helps prevent our adversaries from "gaining" or "exploiting" any unclassified information about our operations. The OPSEC process identifies critical components of friendly information and analyzes friendly actions that accompany military operations and other activities to:

- ✪ Identify those friendly actions that can be observed by adversary intelligence systems;
- ✪ Determine indicators of our operations that adversary intelligence systems might gather that could be interpreted or pieced together to derive critical information in time to be useful; and
- ✪ Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary collection and exploitation.

OPSEC is not a collection of specific rules and instructions that can be applied to every operation; it is a methodology that can be applied to any operation or activity for the purpose of denying critical information to the adversary. Remember, **critical information includes more than classified information. OPSEC aims to identify any unclassified activity or information that when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities.** OPSEC is applied to all military activities, offensive or defensive, at all levels of command. *Air Force commanders at all levels ensure OPSEC awareness and that appropriate OPSEC measures are implemented continuously during peacetime and times of conflict.* Commanders should provide OPSEC planning guidance to the staff at the start of the planning process when stating the "commander's intent" and subsequently to the supporting commanders in the chain of command. By maintaining a liaison with the supporting commanders and coordinating OPSEC planning guidance, commanders can help ensure unity of effort in gaining and maintaining the essential security awareness considered necessary for success.

Information Assurance (IA)

IA comprises those measures to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and nonrepudiation (ability to prove sender's identity and prove delivery to recipient). IA includes the protection of information systems against unauthorized access or information corruption. IA includes the ability to restore information systems by incorporating protection, detection, and reaction capabilities. The IA process is applied through a triad of resources. These resources include our trained people, our systems and technical tools, and our policies and procedures. IA is achieved through the 'defense-in-

depth' concept. Defense-in-depth integrates the capabilities of our people, operations, and technology to achieve strong, effective, multi-layer, multidimensional protection.

IA activities may often be closely integrated with computer network defense and electronic protection activities. In some instances, specific IA, CND, or EP activities may appear to overlap, but again, the important focus for airmen is on integration of these activities, coordination, and desired effects. IA, like CND and OPSEC, is applied to all military activities at all levels of command.

IA encompasses computer security and communications security (COMSEC). It may include other measures necessary to detect, document, and counter such threats.

- Computer security involves the measures and controls taken to ensure confidentiality, integrity, and availability of information processed and stored by a computer. These include policies, procedures, and the hardware and software tools necessary to protect computer systems and information.
- Communications security includes measures and controls taken to deny unauthorized persons information derived from telecommunications while also ensuring telecommunications authenticity. Communications security includes cryptosecurity, transmission security, emission security (EMSEC), and physical security of communications security materials and information.

IA is discussed in further detail in chapter four, Information Services.

Computer Network Defense (CND)

CND is actions taken to plan and direct responses to unauthorized activity in defense of Air Force information systems and computer networks. Commanders should provide CND planning guidance to the staff, as well as supporting and subordinate commanders, as part of the "commander's intent." **CND actions include analyzing network activity to determine the appropriate course of action (COA) to defend Air Force networks.** *Often this task will require fusion with information assurance activities, intelligence information, counterintelligence information, and operational considerations to determine the nature of the threat to friendly systems.* This analysis effort leads to the development of appropriate defensive COAs to the unauthorized activity.

For example, system and network administrators provide routine, continuous application of defense-in-depth through daily-implemented, standing COAs. At any Air Force location, whether it is an action blocking an Internet Protocol (IP) address, employing the latest antivirus tool, or responding through other commander-directed responses, many different people and organizations are involved in the actions and reactions within CND.

In a notional example, distributed electronic sensors and/or human operators would initially indicate Air Force networks are under attack. Next, an analysis of the attack fused with operational considerations would further define the nature of the threat to Air Force systems. This analysis would then assist in the development of a comprehensive range of COAs to the attack. Commanders select the most appropriate COAs, and execute those actions to defend network information and systems. Finally, post-event, additional protection measures may be implemented to counter the specific tactics and techniques used during the attack.

A real-world example of CND of Air Force networks occurred during recent military operations within Air Force networks that came under a variety of attacks, including e-mail flooding and Web page attacks. Air Force Computer Emergency Response Team (AFCERT) personnel responded to these threats by closely monitoring and analyzing the unauthorized activity to determine the intruder's intent and identity. This analysis was in turn used to develop and make recommendations on COAs. In this example, blocking the activity from Air Force networks was the COA adopted.

Counterdeception

Counterdeception is the effort to gain advantage from, or negate, neutralize, or diminish the effects of, a foreign deception operation. Counterdeception requires analysis to develop appropriate COAs to respond to adversary deception efforts. Counterdeception involves the use of other air and space functions, for example, ISR, PSYOP, or physical attack, to create the effects that negate, neutralize, diminish, or gain an advantage from a foreign deception operation. *Early identification of foreign deception activities* can ensure friendly decision makers are aware of adversary deception activities in order to take appropriate action. This awareness comes from a continual analysis of adversary operations for deception activities and is a critical step in counterdeception.

Integrated ISR activities provide awareness of an adversary's posture or intent and also identify an adversary's attempts to deceive friendly forces. As the Air Force develops more near-real-time information processes, methods for identifying adversary deception must extend beyond the traditional intelligence process. While ISR capabilities are critical to counterdeception efforts, ISR analysis is not counterdeception. Further, it is important to understand that personnel trained to perform counterdeception analysis do not conduct friendly military deception operations themselves. They can, however, support friendly deception operations being planned, coordinated, and executed by designated military deception planners.

After identification of an adversary deception operation, commanders can adopt several COAs. *Commanders can ignore, expose, exploit, or eliminate adversary deception efforts*. Each COA involves different levels of risk. For example, ignoring the deception might make sense if acknowledging the deception compromises friendly deception identification capabilities. Such a compromise of friendly capabilities might lead to future improvements in adversary deception capabilities. Commanders might choose to publicly expose the deception to cause embarrassment or to increase an adversary's operational friction. Another COA might be to exploit the adversary's deception effort. An example of exploitation might involve friendly forces pretending to be deceived until the culminating point of the adversary's deception, and then reacting in an unexpected manner. Eliminating the adversary deception effort would involve destroying or degrading the adversary's deception capabilities and resources. Many different air and space capabilities can be used to destroy or degrade deception efforts.

Some counterdeception activities can occur before or after adversary deception operations. Counterdeception activities also include educating friendly forces to adversary deception capabilities or performing damage control through employment of OPSEC measures to deny an adversary feedback on the effectiveness of their deception effort.

Counterintelligence (CI)

CI protects operations, information systems, technology, facilities, personnel, and other resources from illegal clandestine acts by foreign intelligence services, terrorists groups, and other elements. Counterintelligence efforts are both proactive

and multitiered and include the full range of protective measures. Counterintelligence capabilities include:

- Identification of threats through investigations and operations.
- Assessment of threats through reactive and predictive analysis.
- Notification of the threat through ISR processes and counterintelligence products.
- Neutralization and exploitation of threats through investigation and operations.

The Air Force Office of Special Investigations (AFOSI) initiates and conducts all Air Force counterintelligence investigations, activities, operations, collections, and other related CI activities. AFOSI supports IO in four distinct, but interrelated, ways:

- By integrating relevant CI capabilities that work predominantly in the information domain.
- By leveraging preexisting resources and technologies.
- By embedding CI capabilities in relevant US Air Force and DOD organizations.
- By providing the commander a uniquely flexible ability that can quickly transition from direct counterintelligence support to law enforcement.

Finally, counterintelligence capabilities should be fully integrated into all planning and execution efforts. *Counterintelligence personnel should be an integral part of the IW Flight (IWF) and liaise closely with the AOC.*

Counterpropaganda Operations

Counterpropaganda involves those efforts to negate, neutralize, diminish the effects of, or gain advantage from foreign psychological operations or propaganda efforts. Numerous organizations and activities (e.g., ISR activities, public affairs, or other military units and commanders) can identify adversary psychological warfare operations attempting to influence friendly populations and military forces. Countering adversary psychological operations is important to successful friendly operations. Air Force commanders

should use the full range of capabilities to help defeat adversary psychological operations. Commanders at all levels should integrate activities designed to reinforce dissemination of truthful information, to mitigate adversary messages, and to disrupt, degrade, and disable adversary psychological operations. Such efforts might range from specific PA operations to convey accurate information to the targeted audiences and mitigate the intended effects of an adversary's psychological operations, to efforts to physically destroy adversary PSYOP resources and assets.

As an example, countering adversary propaganda is another use of PA operations in an IFDO. *Gaining and maintaining the information initiative in a conflict can be a powerful weapon to defeat propaganda.* The first out with information often sets the context and frames the public debate. *It is extremely important to get complete, truthful information out first—*especially information about friendly forces' mistakes and blunders, so that friendly forces are exposing those errors and putting them into the proper context. Air Force Combat Camera provides on-demand imagery acquisition and multimedia services. Photographic activities cover the full spectrum of air and space functions, notably aerial documentation and editing of weapon system video—the gum camera footage. This will help disarm the adversary's propaganda and defeat attempts by the adversary to use these mistakes for their propaganda value.

Credibility and ground truth are key concepts to fighting adversary propaganda. US and friendly forces must strive to become the favored source of information by the international news media—favored because we provide truthful and credible information quickly.

The credibility and reputation of the US military organization in international news media is a crucial factor in combating adversary propaganda. It is absolutely imperative that this credibility is maintained; otherwise news media and the public may lose confidence in what our spokespersons say. If credibility is not maintained, our operational ability to use PA operations for combating adversary propaganda, for providing informational flexible deterrent options, virtual force projection, or maintaining national will, could be permanently and irreparably damaged. Providing fast, truthful, credible information to the news media is operationally essential in order to maintain this capability.

Adversaries of the United States have used propaganda during many conflicts and most propaganda activities play out through the domestic and international news media. While we may anticipate propaganda being used against US leaders, publics, and armed forces, PA operations may not use propaganda techniques on the US public to combat adversary propaganda. The Smith-Mundt Act of 1948 prohibits PA operations from using propaganda techniques to intentionally misinform the US public, Congress, or US media about military capabilities and intentions in ways that influence US decision makers and public opinion.

Finally it is important to understand that all information operation functions, such as computer network attack, physical attack, PSYOP, PA operations, EW, or ISR can help counter the adversary's PSYOP efforts.

Electronic Protection (Electronic Warfare)

Electronic protection is primarily the defensive aspect of electronic warfare. It is focused on protecting personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. *EA and ES can also play a role in supporting electronic protection efforts.* The goal of EP is to ensure that friendly forces do not suffer the effects of electromagnetic attack from friendly EW operations or hostile EW operations.

Electronic protection might include electronic shielding of sensitive electronic equipment from hostile emissions, frequency deconfliction among friendly systems, or the use of frequency-hopping. Electronic attack to counter hostile electromagnetic emissions can also be seen as a form of electronic protection.

Public Affairs (PA) Operations

Commanders should make PA operations part of their defensive counterinformation planning. PA operations should be coordinated closely with, and can also directly support other defensive IW activities such as OPSEC counterpropaganda efforts and PSYOP. However, it is important to reiterate that legal restrictions and DOD policy make it unlawful to intentionally

misinform the US public, Congress, or media about military capabilities and intentions.

PA operations should be coordinated and deconflicted with other IO activities because communication technology can make information simultaneously available to domestic and international audiences. *The synergistic effects of integrating PA operations into IO planning significantly enhance a commander's ability to achieve military objectives.* For example, PA operations can be the first line of defense against adversary propaganda and disinformation in the news media. As weapons in the commander's arsenal of information operations assets, PA operations can be a force multiplier that both assesses and shapes the information environment's effect on military operations.

CHAPTER THREE

INFORMATION-IN-WARFARE (IIW)

Information-in-warfare is the second subset of information functions within the IO construct. IIW includes the gain and exploit aspects of IO. IIW is a term that identifies air and space power functions designed to continuously **provide commanders situational awareness** across the spectrum of conflict. IIW functions support counterinformation, but it is important to understand that IIW functions also support all other operations as well—around the clock—during peacetime, crisis, or conflict. Conversely, counterinformation activities or other operations may contribute to the success of certain IIW activities.

Critical IIW functions such as ISR, precision navigation and positioning, weather services, information collection and dissemination activities, and PA operations enhance the employment of air, space, and other information operations. Together, these functions provide commanders reliable information that gives them the ability to observe the overall battlespace, analyze events, and maintain awareness. *IIW functions provide commanders with a wide range of actionable, predictive, and valuable information.*

IIW, like IW, relies on the capabilities provided by information services. The interrelationship between IIW and ISvs helps provide our commanders with the right information at the right time. For example, large assets and resources such as the entire communications and information infrastructure; or specific systems like the Airborne Warning and Control System (AWACS) or joint surveillance, target attack radar system (JSTARS); enable commanders to understand the battlespace. Other resources like unmanned aerial vehicles (UAVs); airborne reconnaissance platforms such as the U–2 and RC–135; weather platforms such as the WC–130; and space systems also help shape operations by giving commanders a superior ability to assess events and take appropriate action. For example, space systems help achieve information superiority by providing the stringent information requirements for precise navigation, collecting and disseminating weather information, conducting ISR operations, and providing other essential information capabilities.

The following IIW functions contribute to air and space operations and also serve to help increase overall IO effectiveness.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR)

Intelligence, surveillance, and reconnaissance are the integrated capabilities to task, collect, process, exploit, and disseminate accurate and timely information. ISR is a critical function that helps provide the commander the situational and battlespace awareness necessary to successfully plan and conduct operations. Today, Air Force-operated ISR assets can provide near global sensor coverage. Commanders can use the intelligence information derived from these assets to maximize their own forces' effectiveness by optimizing friendly force strengths, exploiting adversary weaknesses, and countering adversary strengths. *To be fully effective, the ISR process must be integrated into the full range of command and control processes and operations.*

It is important to note that the surveillance and reconnaissance functions of ISR are differentiated by the following definitions: surveillance is continuous collection of information from the air, space, and Earth's surface; reconnaissance is conducted to gain information on localized and specific targets within a constrained time frame. Despite the distinction between surveillance and reconnaissance, collection platforms or teams often conduct surveillance and reconnaissance functions of ISR simultaneously.

Accurate and timely intelligence information derived from the ISR process is an important element in achieving campaign objectives. Today, ISR collection and analysis are conducted constantly. ISR personnel help provide situational awareness, which is essential for monitoring and assessing global conditions. With respect to contributing to friendly IW efforts, Air Force ISR activities seek to obtain a superior understanding of the strengths and weaknesses of an adversary's information systems and infrastructure to provide information vulnerability analysis. Effective and relevant ISR creates opportunities for systematic exploitation of an adversary's liabilities and helps isolate their forces from their leadership. For example, ISR personnel often maintain databases for nodal analysis and assessing foreign military capabilities. The process of fusing disparate pieces of intelligence information from these databases and from a variety of other sources can provide immediate worldwide crisis support for all air and space operations. ISR personnel must now keep the capabilities and

requirements of IO in mind, while maintaining their traditional focus on warfare.

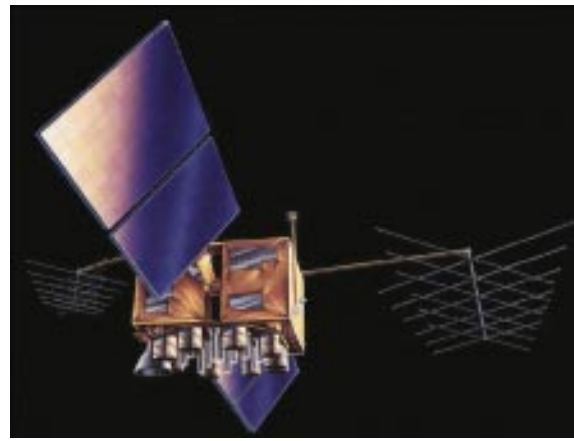
Furthermore, ISR support of IW requires the tasking, collection, and analysis of information about the specific details of an adversary's telecommunications and computer infrastructure—not just a catalog of systems a state or group has in inventory—but also the details of how adversary systems are installed, work, and are used. In addition, intelligence analysts strive to accurately estimate an adversary's probable COAs, including their capability and intentions to conduct IW. Despite a requirement for additional emphasis on adversary IW capabilities, continued ISR effort in traditional areas (such as orders of battle analysis and indications and warning [I&W]) is still required.

A key ISR methodology for providing accurate and timely intelligence information is found in the intelligence preparation of the battlespace (IPB) process. IPB is a systematic, continuous process of analyzing the threat and environment to help the commander better predict, understand, and shape the battlespace. Specifically, *IPB focuses on the interrelationship between threat and environment and the effect on that interaction on both friendly and enemy COAs.* The IPB process provides warfighters with a mission-focused and tailored understanding of an adversary. IPB methods, processes, and products can support air, space, and information operations.

ISR resources and assets help provide I&W and situational awareness of threats to the United States and its allies. Air, space, and land-based ISR systems and capabilities can provide information on orders of battle, disposition, capabilities, and events underway. As an example, space-based ISR systems now provide near global coverage. Air Force, national-level, and some civil space assets offer commanders a responsive information collection capability that supports the decision-making process. Thus, ISR resources should also be seen as a critical part of the GIG.

Finally, airmen need to remember that the synergistic results from ISR operations are essential for all successful operations. **ISR's synergistic effect results from the effective management in a combat environment of surveillance and reconnaissance, as well as intelligence tasking, processing, exploitation, and dissemination operations.**

PRECISION NAVIGATION AND POSITIONING (PNP)



Global positioning systems have revolutionized warfare.

Precision navigation and positioning is another IIW function that constantly supports other air and space operations as well as other IO functions. **PNP gives operators the capability to precisely attack targets in sensitive areas.** The ability to locate a target and then deliver accurate firepower through physical attack, for example, greatly reduces the number of aircraft and sorties required to neutralize or destroy a target. Likewise, PNP support to space operations increases the efficiency of space system operations and helps space systems respond accurately to requests for information. *PNP can also help support IO such as ISR, PSYOP, and EW, for example, by providing accurate coordinates of adversary threat locations.*

PNP capabilities have enhanced the accuracy of both weapons and delivery platforms to the point that weapons can more reliably strike individual (discrete) targets to achieve very specific effects. Many factors contribute to a weapon's ability to be delivered with greater accuracy. Modern aircraft sensors, targeting systems, and precision-guided munitions allow accurate location of targets and delivery of firepower. Space support, integrated intelligence, and precision navigation equipment also allow accurate delivery of unguided ordnance. Air, space, and surface forces armed with PNP equipment are able to attack moving targets in sensitive areas. Users of the global positioning system can process satellite signals and determine position within tens of feet, velocity within a fraction of a mile per hour, and time within a millionth of a second.

WEATHER OPERATIONS

Know the ground, know the weather; your victory will be total . . .

Sun Tzu, 500 B. C.

Air Force weather operations, a basic air and space power function introduced in AFDD 1, provide essential information about the air and space environment to the warfighter.

History has demonstrated that awareness or ignorance of the effects of the air and space environment can have a decisive impact on war. *Environmental information is a critical element of the decision-making process* for employing forces and planning and conducting air, ground, sea, and space operations. In this context, the commander's ability to make good decisions is enhanced by integrating knowledge of the weather into every facet of operations.

Weather operations consist of the capabilities to collect, analyze, predict, tailor and communicate accurate, relevant and timely battlespace information for the warfighter. Weather operations personnel strive to provide *weather information that is focued on the commander's needs and objectives, and can be integrated into the planning process early* to successfully plan and execute military operations. Defining impacts to mission, platforms, weapon systems, targets, tactics, and timing are the focus of weather operations.

Air Force weather operations provide impacts to mission task execution in the air and space environment. This knowledge enables exploitation of the "weather delta"—maximizing friendly forces' strengths and capabilities, exploiting adversary weaknesses and countering adversary strengths. This is critical to operational planning because it can allow commanders to plan friendly operations based on potential adversary COAs after evaluating adversary capabilities in particular environmental conditions. Additionally, weather information can be integrated into OPSEC and deception planning.

Weather operations should be operationally focused and mission tailored. This information should be integrated into all phases of planning and execution to ensure the commander has the opportunity to evaluate the mission from an environmental

perspective, mitigate or exploit its impact, and enable full exploitation of IIW and IW capabilities.

PUBLIC AFFAIRS (PA) OPERATIONS

In addition to its capabilities to help "attack and defend" in the counterinformation operations realm, **PA operations has a vital role across the spectrum of conflict to help "gain and exploit" information.** PA operations *support the warfighter in peace or in war* with a variety of capabilities. Thus, PA operations spans IO by being a function applicable to both information-in-warfare and information warfare. **Commanders should use PA operations to collect and communicate unclassified information about activities to Air Force, domestic, and international communities.** PA operations include, but are not limited to, public affairs, musical programs, broadcasting, visual information, combat camera, recruiting, and history and museum programs. PA operations can assist commanders in four distinct ways across the spectrum of conflict. These four types of support include providing trusted counsel, enhancing airman morale and readiness, enhancing unit cohesion and pride, and building public trust.

One of the key roles of PA operations in both the IW and IIW context is to *provide trusted counsel* to commanders. This capability includes analyzing and interpreting the global information environment, monitoring domestic and foreign public opinion, political controversies, social traditions, and cultural shifts. PA operations can provide lessons learned from the past and prepare leaders to communicate through news media in peace or in war. In addition to supporting a commander's campaign, PA's role as a trusted counselor contributes directly to IO functions such as countering adversary propaganda, ensuring mission OPSEC, and computer or physical attack by helping commanders to make well-informed decisions and to forecast possible results of military operations within the public information battlespace.

PA operations can also *enhance airman morale and readiness.* PA operations can help airmen to understand their roles in the mission and explain how policies, programs, and operations affect them and their families. Because military operations often receive intense news media attention, airmen must fully understand that the decisions they make, what they say, and their actions can have immediate implica-

tions. PA operations can also help fight loneliness, confusion, boredom, uncertainty, fear, rumors, adversary deception efforts, and other factors that cause stress and undermine efficient operations. Finally, PA operations *enhance unit cohesion and pride* by recording and disseminating the record of the unit's historic achievement, accumulated honors, or in some cases, aerial victory credits.

PA operations help support a strong national defense, in effect preparing the nation for war, by *building public trust* and understanding for the military's contribution to national security and its budgetary requirements. With backing from the tax-paying public and Congress, military leaders are able to effectively recruit, equip, and train airmen to perform across the full spectrum of military operations. During national crisis, this capability gives the American public the information they need to understand the importance of military action—in effect, bolstering national will. This kind of communication gives commanders an option that allows them to "get in front" of a crisis, influence the perception of events, clarify public understanding, and frame the public debate.

Commanders may employ PA operations to develop and implement communication strategies targeted toward informing national and international audiences about air and space power's impact on global events. Making international audiences aware of forces being positioned overseas and US resolve to employ those assets through tactics such as a *"virtual force projection"* can enhance support from friendly countries. The same information may deter potential adversaries, driving a crisis back to peace before use of force becomes necessary. When adversaries aren't deterred from conflict, information revealing US or friendly force capabilities and resolve may still affect adversary decision makers. Communicating military capabilities to national and international audiences can be a *force multiplier.*

PA Operations Planning

Commanders should make PA operations part of their information operations planning. PA operations should be coordinated closely with, and can also play a direct part in, IW activities such as counterpropaganda, OPSEC, and PSYOP. **The synergistic effects of integrating PA operations into IO planning significantly enhance a commander's ability to achieve military objectives.** Coordination

and deconfliction will ensure that the credibility of US operations and communications is retained. Otherwise, public trust and support for the Air Force could be undermined or lost.

Combat Camera Operations

One key aspect of PA operations includes combat camera capabilities. **Commanders may use combat camera as a tool to communicate classified and unclassified still and motion imagery documenting operations to Air Force leaders and joint force commanders. Combat camera imagery may also be used to support other PA operations in informing domestic and international audiences, but its primary use is as an IIW decision-making tool.** Combat camera can be a force multiplier that documents the combat information environment and delivers the **critical imagery for the commander** to use in decision making.

CHAPTER FOUR

INFORMATION SERVICES (ISvs)

Information operations provide the means to rapidly collect, process, disseminate and protect information while denying these apabilities to adversaries. Information operations represent a critical capability enhancement for transformed U.S. forces.

Quadrennial Defense Review
September 30, 2001

Creating and leveraging information superiority is essential to the conduct of successful operations—from peacetime through all levels of conflict. **Fundamental to achieving information superiority is the DOD's Global Information Grid (GIG).** The GIG is designed to achieve a seamless, secure, and coherent 'infostructure' for full spectrum voice, data, and video demands. Attributes of the GIG—protected, assured, interoperable communications—are essential to information superiority.

Air Force information services (ISvs) provide the infrastructure, communications pathways, computing information services power, applications support, information management, and network operations to make the GIG a reality. Elements of the Air Force's ISvs include: information assurance; applications; spectrum management; information resources management; establishment, operation, and sustainment of networks; and information technology infrastructure. ISvs are a critical part of the Air Force's effort to achieve information superiority. For example, ISvs provide the underpinnings for reachback capabilities, tight sensor-to-shooter links and distributive collaborative planning tools. *The result of optimized information services is confidence in the integrity and reliability of available information—a prerequisite for information superiority.*

INFORMATION ASSURANCE (IA)

IA is a vital requirement of the Air Force's operational readiness and it ensures continuous and dependable information is provided through the other ISvs components. IA depends on the continuous integration of trained personnel, operational and technical capabilities

and necessary policies and procedures to guarantee *availability, integrity, authenticity, confidentiality, and nonrepudiation* of information services, while providing the means to efficiently reconstitute these vital services following disruptions of any kind, whether from an attack, natural disaster, equipment failure, or operator error. In an assured infostructure, warfighters can leverage the power of the Information Age.

Developing and implementing security and protection in the twenty-first century requires recognition of the globalization of information and information systems. The Air Force employs a defense-in-depth philosophy by providing layered and integrated protection of information, information systems, and networks. The defense-in-depth approach employs and integrates the abilities of people, operations, and technology to establish multilayer, multidimensional protection. The rigorous defense-in-depth approach strengthens our security posture and ensures information vital to our expeditionary operations is timely, accurate, and reliable. Security and protection include the policies and programs to help counter internal and external threats—whether foreign or domestic—to include protection against trusted insider misconduct or error. Security, like interoperability, must be incorporated into information systems designs from the beginning to be effective and affordable. Level of protection must be commensurate to the importance and vulnerability of the specific information and information systems.

Traditional programs such as COMSEC and emissions security as well as CND are methods to protect our information and information systems. In addition, other information assurance programs help assess the interoperability, compatibility, and supportability of our information systems and aim specifically to reduce vulnerabilities and to improve the overall security of networks and systems shared by all.

The following five components of information services—properly *implemented, operated, maintained, protected, and defended*—result in IA and provide critical enabling underpinnings to IO and information superiority as well as to the other five core competencies.

APPLICATIONS

Many information products presented to operators and decision makers are derived from software programs. The information products and the software that helps produce them are often referred to as applications.

Modern applications address many needs: from database tools that store, manipulate, and retrieve information to the software that ties together ground, air, and space-based command and control (C2) and combat support systems. Using real-time and historical data, supporting analysis, and operational risk assessments, well-developed applications enable better decisions to be made as quickly as conditions demand. To illustrate the point, properly developed and implemented C2 and combat support applications enable us to operate inside an adversary's decision loop.

SPECTRUM MANAGEMENT

The Information Age has intensified universal demands on the electromagnetic spectrum. The spectrum is internationally recognized as a natural resource within the boundaries of every sovereign nation. *Consequently, governments now treat the electromagnetic spectrum as a national asset and tightly regulate access to it within their national boundaries for economic and security reasons.* Access to the electromagnetic spectrum is vital to sustaining forces. It is as critical to the proper employment of air and space power as jet fuel or bombs. Rigorous planning must be accomplished at all levels of command during peace and conflict to ensure that mission critical elements of the electromagnetic spectrum are available.

INFORMATION RESOURCE MANAGEMENT (IRM)

Simply put, **IRM is the process of managing information resources to accomplish the mission.** Successful IRM is measured at the point of need: the operator or decision maker is presented with information matched to the task at hand. *To ensure the appropriate information is available for delivery to the appropriate user, the Air Force treats information as a strategic resource throughout its life cycle (from acquisition or creation through disposition, including protection and access for storage, retrieval, use, and distribution).*

ESTABLISHING, OPERATING, AND SUSTAINING NETWORKS

Parallel to development, operations, and maintenance of Air Force weapons systems, information networks must be established, operated, and sustained. Air Force owned and supported networks provide a spectrum of services to include data, voice, and video, both wired and wireless. Optimal network operations can be

achieved by effectively and efficiently addressing performance management, configuration management, change management, operating systems management, help desk tools and services, service scheduling, and backup and recovery management. However, airmen cannot afford to pursue optimal network performance by sacrificing necessary security measures. *Commanders should seek the best balance between network security and efficient network operations through the use of risk management.* Balancing these sometimes conflicting needs demands knowledgeable, well-informed commanders, highly skilled personnel equipped with the proper technical expertise, and the resources to ensure the Air Force has robust, effective, and assured communications and information networks.

The Air Force accomplishes network operations by employing a three-tiered Enterprise Network Operations management structure consisting of the:

- Network Control Centers (NCCs) at base level
- Network Operations and Security Centers (NOSCs) at the major command (MAJCOM) level
- Air Force Network Operations Center (AFNOC) and the Air Force Computer Emergency Response Team (AFCERT) at the Air Force level

These three levels of AF network operations provide commanders with the real-time visibility, management, and control of networks that are crucial to information assurance and to Air Force mission success.

Network Control Center (NCC)

The NCC oversees network operations, helps achieve information assurance, and generates visibility into the base network. Wing and theater air base commanders exercise command and control over their fixed base or deployed site networks and systems via the NCC. Using network management, intrusion detection, and vulnerability assessment tools, the NCC technicians provide flexible and scaleable levels of service to functional system administrators, workgroup managers and users 24 hours per day, 7 days per week.

Network Operations and Security Center (NOSC)

Commanders should play an active role in the support and management of network activities within their operational areas. **A NOSC provides commanders with real-time operational network intrusion detection and perimeter defense capabilities, as well as theater-level network management and fault resolution activities.** This dedicated first-line of defense is employed at the commander's direction to defend information networks both in-theater and in-garrison. Equipped with advanced systems, a NOSC can deploy automated equipment and augmentation forces in theater, as needed, to perform CND and information assurance operations. NOSCs provide data fusion, assessment, and decision support. To accomplish this, they often have many of the systems and tools identical to those supporting the AFCERT. NOSC personnel monitor and support the day-to-day operational issues associated with their subordinate bases and units. Their mission focus is to ensure their command's operational and support systems are fully capable. As appropriate, they support their commanders with information assurance capabilities, such as information systems security, decision analysis, and other technological capabilities. *Finally, support from the NOSC and Network Operations and Security Center (Deployable) (NOSC-D) are essential to the IW Flight.* The support provided from NOSC personnel helps develop some DCI COAs. These COAs will contribute to the strategy to achieve the commander's air and space objectives.

Air Force Network Operations Center (AFNOC)

The AFNOC is the Air Force's top network management tier. **This top-tier organization provides senior leaders the network enterprise view across the Air Force.** One of its primary roles is to manage base-level service delivery point network routers to produce global visibility of the Air Force's enterprise network and critical applications. **The AFNOC monitors and responds to anomalies in communications and information networks, systems, and applications in coordination with the Defense Information Systems Agency, MAJCOMs, and the commercial sector.** The AFNOC also operates in concert with the AFCERT to provide strong computer network defense capability to Air Force networks. Lastly the AFNOC manages or oversees enterprise helpdesks to provide flexible and scaleable levels of service to NOSCs and bases 24 hours per day, 7 days per week.

INFORMATION TECHNOLOGY (IT) INFRASTRUCTURE

To help achieve and maintain a position of information superiority over existing and potential adversaries, the Air Force infrastructure supporting the GIG should adopt applicable leading edge IT. This should be done while maintaining a focus on IT interoperability and sustainability as well as the effects on those charged with its employment and maintenance. Our strategies for constructing and implementing the Air Force Information Technology Infrastructure should be extremely flexible and responsive. To ensure the right information technology is properly incorporated into the GIG, we must do two things (in this order):

- Reengineer mission processes to best meet mission requirements
- Carefully match the appropriate information technology to those reengineered processes

In other words, we must not only apply technology to today's processes, but airmen should use the opportunities information technology provides to do things smarter and more efficiently tomorrow.

CHAPTER FIVE

INFORMATION OPERATIONS IN THEATER OPERATIONS

We need to be able to think in terms of target effects. I picture myself around that same targeting table where you have the fighter pilot, the bomber pilot, the special operations people and the information warriors. As you go down the target list, each one takes a turn raising his or her hand saying, "I can take that target."

General John P. Jumper
Commander, US Air Forces in Europe
Defense Colloquium on Information Operations
March 25, 1999

INFORMATION SUPERIORITY

One of the commander's priorities is to achieve information superiority over an adversary by controlling the information environment. This goal does not in any way diminish the commander's need to achieve air and space superiority but rather facilitates efforts in those areas and vice versa. The aim of information superiority is to have greater situational awareness and control over the adversary. Effective use of IO leads to information superiority. **The effort to achieve information superiority depends upon several fundamental components: an effects-based approach, superior battlespace awareness, well integrated IW and IIW planning and execution, and information operations organizations.** The following paragraphs discuss these important components.

EFFECTS-BASED APPROACH

Fundamental to the Air Force's success in the next century is its ability to focus on the effects necessary to achieve campaign objectives, whether at the strategic, operational, or tactical levels. **An effect is the anticipated outcome or consequence that results from a particular military operation.** The emphasis on effects is as crucial for successful IO as for any other air and space power function. *Commanders should clearly articulate the objectives, or goals, of a given military operation. Effects should then flow naturally from objectives as a*

product of the military operations designed to help achieve those objectives. Based on clear objectives, planners should design specific operations to achieve a desired outcome, and then identify the specific optimum capability for achieving that outcome. *Critical to the effects-based approach is the requirement to be able to measure IO effects; this 'feedback' allows the commander to evaluate IO and adjust specific information operations to evolving combat situations to increase its effectiveness.* The following sections provide examples of the types of effects IO can achieve and provide a brief review of the targeting process.

Strategic Effects

Strategic effects can be created by a wide variety of military actions occurring at all levels of war. **Most OCI and DCI information operations at the strategic level of war will be directed by the NCA and planned in coordination with other agencies or organizations outside the DOD.** Such operations should be **coordinated among supporting Air Force units,** the combatant commander's IO team or cell, and other supporting components, if present, to ensure unity of effort and prevent conflict with possible ongoing operational-level operations. However, due to the sensitivity of such operations, they may not always be coordinated with other units, but rather synchronized and deconflicted at the highest level possible to ensure fully integrated, successful operations. *Nevertheless, information operations at the strategic level of war may also be conducted as part of normal theater operations.* Specific effects IO can achieve at this level are:

- Provide global situation awareness in near real time.
- Influence both friendly and adversarial behavior conducive toward achieving national objectives through the promotion of durable relationships and partnerships with friendly nations.
- Institute appropriate protective and defensive measures to ensure friendly forces can continuously conduct IO across the entire spectrum of conflict. Such measures create effects that deny adversaries knowledge of, or ability to access or disrupt, friendly information operations.
- Reduce adversary leadership resistance to US national objectives by affecting willpower, resolve, or confidence. Create a lack of

confidence in an adversary's military, diplomatic, or economic ability to achieve its goals or defeat US goals.

- Negatively impact an adversary's ability to lead by affecting their communications with their forces or their understanding of the operating environment.

- Deter aggression, support counterproliferation of weapons of mass destruction, support homeland defense, and support counterterrorism.

- Employ actions that reduce friendly vulnerabilities to physical and cyber attacks on our information and information systems through proactive and layered protective and defensive measures.

Operational Effects

Operational effects can be created by a wide variety of military actions occurring at all levels of war. **IO at the operational level of war can be conducted by CINCs and the Commander, Air Force Forces (COMAFFOR) within their assigned area of responsibility or joint operation area at home or abroad.** IO at this level will involve the use of military assets and capabilities to achieve operational effects through the design, organization, integration, and conduct of campaigns and major operations. IO plans between and among supported and supporting commands should be coordinated closely to prevent redundancy, mission degradation, or fratricide. Specific effects IO can achieve at this level include:

- Provide commanders with increased awareness of, and influence over, the battlespace. This is done through gaining, exploiting, and disseminating accurate, reliable, and near-real-time information.

- Hinder an adversary's ability to strike. Incapacitate their information-intensive systems. Create confusion about the operational environment.

- Slow or cease an adversary's operational tempo. Cause hesitation, confusion, and misdirection.

- Reduce an adversary's command and control capability while easing the task of the war-to-peace transition. Nonlethal counterinformation techniques can be used instead of physical attack. These kinds of activities can preserve the physical integrity of some targets for later

use and can reduce or prevent reconstruction costs during the war-to-peace transition.

- Influence adversary and neutral perceptions away from adversary objectives and toward US objectives thereby inducing surrender or desertion.
- Enhance US plans and operations by disrupting adversary plans.
- Disrupt the adversary commander's ability to focus combat power.
- Influence the adversary commander's estimate of the situation. By creating confusion and inaccuracy in the assumptions an adversary makes about the situation, the direction and outcome of adversary military operations can be shaped.
- Employ actions that reduce friendly vulnerabilities to physical and cyber attacks on our information and information systems through proactive and layered protective and defensive measures.

Tactical Effects

Tactical effects can be created by a wide variety of military actions. Air Force component or functional air and space component commanders direct the execution of tactical-level IO. **The primary focus of IO at the tactical level of war is to deny, degrade, deceive, disrupt, or destroy an adversary's use of information and information systems relating to C2, intelligence, and other critical information-based processes directly related to conducting military operations.** Specific effects:

- Improve the commander's situational awareness and view of the battlespace at the tactical level. Find, fix, track, target, engage, assess, and classify significant military targets.
- Deny, degrade, disrupt, deceive, or destroy adversary capabilities and information on friendly forces.
- Destroy enemy's capability to communicate.
- Reduce the capability of adversary forces.
- Deny adversary knowledge of forces.

✪ Protect friendly information and information systems to give friendly forces the ability to leverage information to accomplish the mission.

Targeting

The purpose of targeting is to achieve specific, desired effects at the strategic, operational, and tactical levels of war. A target is a specific area, object, person, function, or facility subject to military action. A target is the 'thing' on which we want to create an effect. Targeting is a comprehensive and involved process of matching 'things' with weapons. It involves recommending to a commander both the things that when attacked will help achieve the commander's objectives and the **best weapons (lethal or nonlethal, kinetic or nonkinetic) to achieve a desired effect.** The targeting process cuts across organizational and traditional functional boundaries. Reachback, liaison, and coordination with organizations possessing nonkinetic capabilities, such as JPOTL or USSPACECOM, is essential. Functional areas such as operations, intelligence, space, logistics, and communications must be closely integrated throughout the targeting process. Close coordination, cooperation, and communication among the participants are essential.

Targeting integrates intelligence information about the threat, the target system, and target characteristics with operations data on friendly force posture, capabilities, weapons effects, objectives, rules of engagement, and doctrine. Targeting matches objectives and guidance with inputs from intelligence and operations to identify the forces necessary to achieve the objectives. Although often confused with just 'weaponeering,' targeting looks across the range of military capabilities. *It spans nuclear, conventional, and nonlethal force application and can also include information warfare, space, and special operations in joint and multinational operations.*

Targeting Process Phases

The first phase of the targeting process is called the objectives and guidance derivation phase. Clear objectives and the commander's guidance are the foundation of the targeting process. Quantifiable and clear objectives and guidance are best for effective operations. Objectives are developed at the national, theater, and component levels. The commander's guidance is generally also

provided from commanders at the national, theater, and component levels. In this phase, the objectives and guidance are developed and disseminated to the targeting cell within the AOC.

The second phase of the targeting process is the target development phase. This involves the examination of potential target systems and their components to determine criticality and vulnerability to attack. *This phase translates the commander's objectives and guidance into a potential list of things to attack*. The product of this phase is a suggested target list with recommended priorities assigned and extent of damage desired.

In the third phase of the targeting process, weaponeering assessment, planners estimate the *types and quantity of weapons needed to achieve a desired tactical effect on individual targets.* The product of this phase is a list of recommended weapons and aircraft for each target and a validated list of weapon impact points for each target. Weaponeering takes into account target vulnerabilities, weapons effects and reliability, delivery accuracy, and delivery conditions, as well as damage criteria.

The fourth phase of the process is called the force application phase. This phase uses the information generated in the target development and weaponeering assessment phases to determine the best force necessary to meet the commander's objectives. At this point, the decision maker is provided *with fused intelligence on the target and weapon systems recommendations. Integration of kinetic and nonkinetic weapons may be required to conceal nonkinetic capabilities.*

Execution planning is the fifth phase of the process. In this phase, planners prepare input for and support the *actual tasking, construction, and subsequent execution by weapon systems.* Input includes data concerning the target, weaponeering calculations, employment parameters, and tactics. The commander is responsible for monitoring the air tasking order (ATO), making any changes necessary, and providing support to the units.

The final phase of the targeting process is called the combat assessment phase. *After mission execution, the process is evaluated.* Improvements in force employment, munitions design, and situation assessments emerge from this appraisal of poststrike data. The results of

this effort affect future combat operations and can change theater objectives.

SUPERIOR BATTLESPACE AWARENESS

Battlespace awareness is a result of, and a contributor to, effective IO. **Battlespace awareness is the result of continuous information gathering and analysis, using a variety of information-in-warfare functions.** It also contributes to the planning and execution of other IO functions by giving commanders the insight into the operational environment in which they will employ other air and space power capabilities. Therefore, integration of IIW functions into the planning, execution, and feedback phases of air and space operations improves battlespace awareness and enables more effective operations. It is important to remember that while the following discussion focuses on the ISR division, *other important IIW functions represented by specialty teams or liaison officers also contribute to battlespace awareness in the AOC.*

IO ORGANIZATIONS

A number of Air Force organizations contribute to effective IO. The following pages discuss several of the key organizations employed in information operations.

ISR Division

The ISR division is a recently developed organizational concept that the commander can use to help integrate ISR, one of the IIW functions, into his war-fighting organization—the AOC. Further, using an ISR division within the AOC structure is another way in which integrated IO planning and integration is conducted. In all circumstances, war-fighting commanders have the latitude as commanders to organize their war-fighting staffs to best meet the JFC's or CINC's objectives assigned them.

The division chief of ISR (CISR) has overall responsibility for all ISR planning, integration, and assessment within the AOC. **The CISR provides unity of effort by unifying all ISR analytical inputs for the commander and should be the commander's focal point for all of the AOC's enemy-focused analytical efforts.** The CISR should

be a senior officer experienced in intelligence, surveillance, and reconnaissance. The ISR division integrates numerous cross-functional disciplines and provides direct support to the other AOC divisions to assist their core processes. ISR activities also support the overall assessment of how air and space operations meet the JFC's broad objectives. Further, the ISR division provides intelligence support to subordinate combat and combat support forces.

The ISR division helps the commander build the *reconnaissance, surveillance, and target acquisition (RSTA) ATO annex.* The RSTA annex, issued by the JFASCC, amplifies the ATO by providing specific ISR sensor tasking and by directing the processing, exploiting, and disseminating procedures. It should include combat assessment criteria and associated measures of effectiveness (MOEs). During planning, the RSTA annex and the Master Air Attack Plan (MAAP) efforts must be integrated to allow the full range of collection assets—national, theater, and tactical—to be integrated to support the JFC's operations. In general, the RSTA annex tasks ISR collection platforms and it provides direction to exploitation centers to ensure the commanders prioritized informational needs are satisfied. Finally, if an ISR division is designated, the RSTA annex will help coordinate target development and combat assessment assistance with the IW Flight concerning IW objectives, priorities, and alternatives.

The ISR division is typically comprised of three main elements: the ISR strategy element, ISR plans element, and the ISR operations element. All three elements help provide threat analysis, targeting support, and battlespace awareness to the various AOC divisions they support. During operations, the ISR strategy element assesses ISR strategy effectiveness and integration into the overall battle plan and helps perform allocation of resources and operational/combat assessments.

The ISR plans element assists in planning ISR operations and integrates them into the ATO. The ISR plans element also ensures the various commanders' information requirements are translated into an effective daily RSTA annex. This ensures an integrated effort takes place among platform management (ATO/airspace control order [ACO]) planners and the tasking, processing, exploiting, and disseminating units. The ISR plans element also coordinates nomination of guarded frequencies

and targets for inclusion in the Joint Restricted Frequencies List and No-Strike List respectively.

The ISR operations element is embedded within the Combat Operations Division and directly supports the chief of Combat Operations. The element is responsible for dynamic battle management of all ISR assets assigned or made available to the commander. Its efforts focus on adjusting ISR assets to fulfill changing commander's guidance, or focus on responding to the dynamics of the modern battlespace; for example, time-sensitive targeting and theater missile defense (TMD) support.

IW Flight (IWF)

The IWF is one of the commander's key IO organizations in the AOC and is one of the main organizational structures through which integrated counterinformation planning and execution are conducted. While the ISR elements in the AOC provide primary intelligence support to the commander about the full range of adversary military capabilities and intentions, the commander maintains awareness of an adversary's information infrastructure, capabilities, and information operations principally through an IWF.

In most cases, the IWF resides within the AOC and may be referred to as the 'IW specialty team.' In a few instances, an IW Flight may support air and space operations through other AOC-like organizations (the tanker airlift control center for example). Based on the commander's direction and guidance, the IW Flight may also design and execute portions of the campaign that rely on IW activities to accomplish the commander's objectives. The IW Flight is primarily focused on counterinformation operations and may plan and help integrate both OCI and DCI operations into the commander's air and space operations. The IIW functions of information operations will often be represented in the AOC by other divisions, a specialty team, or by individual expertise imbedded in the AOC divisions.

An Air Force IWF (or IW specialty team) should work as an integral element within the AOC to help integrate Air Force IW activities into a joint air and space operations plan, ATO, and space tasking order. The IW Flight's efforts should be fully

integrated with the Strategy, Combat Plans, Air Mobility, Combat Operations, and ISR Divisions in the AOC.

The flight is composed of experienced information operators drawn from many IO disciplines. The IWF should include dedicated ISR personnel and communications support distinct from personnel working in an ISR division or specialty team, or communications support elements within the AOC. *The IWF collects and disseminates information, analyzes information, develops counterinformation COAs, coordinates counterinformation activities, and helps integrate their execution into air and space campaign plans.*

The IWF is normally associated with a special technical operations (STO) cell that will coordinate with other Service, joint, and national-level agencies to insure appropriate planning and coordination for STO activities occurs and is fully integrated with other operations. Some IWF members may work within the STO cell.

An IWF should have permanent members and may be augmented by additional personnel, as the situation requires. Permanent members have no other responsibilities in the AOC, are experienced in their position, and should have specific IO training. Other assistance comes from principal members, temporary members, and liaison personnel. Principal members are experts within their functional area, who are required for the IWF's mission and stay with the team, but may have other AOC responsibilities. Temporary members contribute special expertise as the need arises, while liaison personnel can help coordinate the IWF's activities within the AOC or among other organizations.

The IWF's planning efforts must be fully integrated into the overall air and space campaign plan. *The IWF develops IW COAs based on COMAFFOR-assigned tasks from JFC objectives.* The resulting plan should include both defensive and offensive counterinformation actions. A successful counterinformation plan contributes to the security of friendly forces by bringing an adversary to battle on friendly forces' terms, seizing and maintaining the initiative, ensuring agility, contributing to surprise, isolating adversary forces from their leadership, and creating opportunities for a systematic exploitation of adversary vulnerabilities. **The key to successful counterinformation operations is full integration of information**

warfare activities throughout the planning, executing, and terminating phases of all joint and multinational operations.

This requires coordination among all in-theater operations, including organizations providing reachback support. When the JFASCC is not an Air Force officer, the COMAFFOR also ensures coordination among OCI and DCI actions both internally and externally with other joint force IO organizations. Air Force information warfare capabilities should be considered as an integral part of the Air Force force, and integrated into the overall theater campaign, not just as an add-on, but as a primary capability the Air Force brings to the conflict.

This normal coordination and integration process within a joint task force is highlighted below:

- The JFC develops theater campaign objectives and will normally *designate a "joint force" IO officer to accomplish broad IW oversight functions.* The joint force IO officer heads the JFC IO team or cell, when designated.
- *The JFC IO team/cell* (composed of select representatives from each staff element, Service component, and supporting agencies responsible for integrating the capabilities and disciplines of IO) *derives campaign IW objectives from JFC guidance.* These objectives may be broad or specific, but should not direct the details of execution. Detailed execution is left to the components to accomplish. This process adheres to the Air Force tenet of centralized control and decentralized execution. This means that the commander should set the priority, effects, and timing for all IW operations.
- *Service components address campaign IW objectives and the effects required* to achieve them. Primary and supporting components are designated by the JFC.
- The IWF takes air component tasks, as determined by the JFC's objectives and commander's intent, for planning and integration. *The IFW helps integrate counterinformation capabilities into the ATO.*
- The IWF should hold *IW coordination meetings* regularly to develop and coordinate COAs to present to the commander for approval. The JFC IO team or cell may serve to deconflict Service component operations COAs if required.

- If the commander's COAs are approved, *the IWF helps integrate them into the ATO or tasking process by coordinating with the Strategy, Combat Plans, and Combat Operations Divisions in the AOC.* If a COA is not approved, it is either terminated or shelved for future consideration.
- The IWF should *ensure the rules of engagement and IW operating requirements and authorizations, such as special target lists, are taken into consideration.* The flight should coordinate IW-specific intelligence requests and requirements and stay in contact with the appropriate assets to resolve problems and coordinate requirements and taskings. Likewise, the IWF chief should help ensure target deconfliction with the Combat Plans and Combat Operations Divisions.

Finally, the IWF performs many IW noncontingency activities for the commander. The IWF contains the IW subject matter experts and should continuously perform certain activities such as IW intelligence prep of the battle space (IPB) and monitoring adversary situational awareness. The IWF, along with other MAJCOM organizations, may also help advocate IW requirements to USAF. **During peacetime, the IWF works continuously with Service, joint, and national-level organizations to ensure their readiness to support the AOC wartime missions.**

Offense-Defense Integration

Successful military operations must carefully integrate both OCI and DCI elements. An integrated approach, combining all the tools, disciplines, and capabilities of counterinformation as needed and appropriate, will yield the best long-term effects. Commanders use their operational judgment to determine the best approach for the counterinformation contribution to the air and space campaign. Commanders should ensure their staffs carefully consider both the advantages and disadvantages of specific OCI and DCI functions in their scheme of maneuver.

OCI and DCI must be deconflicted and priorities established. Operational commanders are responsible for such decisions, under the guidance of higher-level campaign plans and, when appropriate, the NCA.

✪ IW Targeting

IWF planners should recommend targets that IW can be used against to support the theater campaign plan. Targeting adversary IW capabilities begins with the commander's intent and involves a strategy-to-task methodology that considers the current legal and political guidelines and rules of engagement. Following these instructions, the targeting process relies on clearly delineated national, theater, and command objectives and the effects required to achieve them to devise a maximum payoff for each course of action. JFCs establish broad planning objectives and guidance for attack of an adversary's strategic and operational centers of gravity. JFCs also plan the defense of friendly strategic and operational centers of gravity as an integral part of joint campaigns and major operations. *The IWF evaluates information target systems, functional relationships, and friendly and adversary critical nodes and recommends appropriate OCI and DCI missions for inclusion in the ATO.* In the weapon assessment and force application stage of targeting, target vulnerabilities are matched with weapons characteristics to produce IW target nominations. Those personnel involved in formulation and evaluation of IW objectives should have access to sensitive information required to help formulate and evaluate those objectives.

The IWF, in coordination with the Combat Plans Division, integrates IW (counterinformation) target nominations into attack plans and tasking orders. Using JFC guidance, apportionment, and the approved target list, the MAAP team provides details on the execution of this guidance using available resources. The ATO and ACO production team converts the MAAP into a tasking in the ATO and the associated special instructions.

Finally, it is important to remember that there are fundamental legal considerations that must be taken into account during all aspects of IW planning and execution, especially with regards to CNA. Commanders should consult with their judge advocate general advisors to assess these legal considerations. Examples of these considerations might include the transition from defense to offense, traditional Laws of Armed Conflict, as well as applicable treaties and agreements.

Network Operations and Security Center (Deployable) (NOSC-D)

As noted in an earlier chapter, **the NOSC provides the commander with real-time operational network intrusion detection and perimeter defense.** Like an in-garrison NOSC, a NOSC-D is a deployable NOSC that is employed at the commander's direction to protect deployed information networks in-theater. A NOSC-D can deploy automated equipment and augmentation forces in theater, as needed, to help perform information assurance and CND operations. *During contingency operations, the NOSC-D should fully coordinate its activities with the IWF.* The IWF will take the lead in recommending IW rules of engagement, offensive COAs, and defensive COAs in response to an attack on information systems. This will be done in close coordination with the NOSC or NOSC-D.

Computer Emergency Response Team (CERT)

Each of the Services has a CERT that responds to computer incidents for their garrisoned and deployed Service forces. In some cases a CERT may directly support a CINC or subordinate joint forces within the CINC's area of responsibility or joint operating area. The Air Force CERT (AFCERT) was established as the single point of contact in the Air Force for computer security incidents and vulnerabilities. **The AFCERT is the lead Air Force organization dedicated to computer network defense.** *The AFCERT, led by the COMAFFOR-CNO, is the Air Force component assigned to Joint Task Force CNO.* The AFCERT assesses, analyzes, and provides countermeasures for computer security incidents and vulnerabilities reported by monitoring equipment, by the Air Force Network Operations Center, the NOSCs, and other agencies. The AFCERT, is responsible for the defense of Air Force networks against computer network attack and exploitation. The AFCERT conducts operations 24-hours per day, 7 days per week to preserve the availability, integrity, and confidentiality of the Air Force enterprise network and information systems. To accomplish this mission, the AFCERT serves as the Air Force OPR responsible for incident response and countermeasure generation for incidents that traverse multiple MAJCOMs or meet/exceed current Air Force incident thresholds. The AFCERT also identifies vulnerabilities, validates and analyzes incidents, provides correlation services, generates risk reduction countermeasures, and collects, compiles, assesses, and reports unauthorized network activity and security incident statistics. The AFCERT works with the AFNOC,

MAJCOM NOSCs, and bases in eradicating malicious logic from a network and/or information system and assists in assessing the scope of unauthorized network activities and incidents. The AFCERT is the Air Force OPR to register, acknowledge, and track implementation of DOD CERT Information Assurance Vulnerability Alerts as defined in DOD directives.

Air Force Information Warfare Center (AFIWC)

The AFIWC was activated in 1993 as the single Air Force focal point for IW activities. The center was established to ensure combatant commanders have the IW capabilities needed to accomplish all offensive and defensive counterinformation missions. **The AFIWC creates the information warfare advantage by exploring, developing, applying, and transitioning counterinformation technology, strategy, tactics, and data to control the information battlespace.**

Through its subordinate organizations, the AFIWC integrates advanced tactics, training, technologies, and tools, arming America's warfighters with decisive IW combat power. The center provides innovative full spectrum counterinformation capability for the Air Force through IW tactics, techniques, and procedures (TTP) development, counterinformation warfighter training, and IW weapons integration. In addition, the AFIWC identifies and provides solutions to Air Force vulnerabilities through Red Team operations. The center's mission includes providing EW analysis, flagging, and reprogramming to warfighters and serves as the Air Force focal point for military deception, counterdeception and psychological operations integration. Furthermore, the AFIWC conducts test and evaluations for emerging IW technologies.

Finally, the AFIWC analyzes US and adversary IO vulnerabilities, explores leading-edge technologies, prototypes solutions, develops concepts and data applications, and migrates information capabilities to warfighters.

Other Reachback Support

Commanders and their staffs should consider all the resources and capabilities available through reachback methods. There are many Service, joint, DOD, or national agencies or organizations listed earlier in this publication that can provide additional support to theater IO

efforts. The IWF and the ISR division should be the main avenues through which to approach these other organizations for additional support.

CHAPTER SIX

TRAINING AND EDUCATION FOR INFORMATION OPERATIONS

While education and training are linked in application, they are distinct in purpose, with each producing markedly different results. In essence, education teaches broad concepts and communicates information upon which to base decisions, whereas training teaches skills necessary to accomplish a task. An Air Force member's education emphasizes critical thought, enabling sound decision making regardless of the situation, while the airman's training provides the skills necessary to master Air Force core competencies.

Major General Ronald E. Keys
United States Air Force

EDUCATION

Training and education of IO forces are an important part of conducting effective information operations. IO operators should have at a minimum a general understanding of all capabilities found within the various IO functions. IO personnel should be thoroughly trained in the specific IO processes that relate to their particular field of expertise. IO personnel should recognize the contribution their functional specialty makes through the strategy of information operations to help achieve the goal of information superiority. The intent of IO education and training is to ensure Air Force IO operators clearly understand the principles, concepts, and characteristics of information operations.

Finally, while not every airman needs a comprehensive course in information operations, *every airman should understand that IO is a key enabler of the Air Force core competency of information superiority and an integral part of air and space power.*

TRAINING AND EXERCISES

Information operations encompass many Air Force specialties performing widely varying functions. Therefore, individual training progression is best left to specialty experts. As Air Force operators, **IO professionals need to receive initial qualification training**

within their assigned specialty and then follow-on on-the-job training at the unit level. Other training that helps experienced specialists plan and execute integrated information operations is also available.

Realistic IO training provided through exercises is essential to proficiency and readiness. Exercises train individuals, units, and staffs in the necessary skills and tools for information operations and ensure that staffs can plan, control, and support such operations. Planners should create realistic and challenging field training exercises, modeling and simulations, seminars, and command post exercises that allow commanders, staffs, and units to participate in information operations. Exercises should emphasize employment operations, as well as deployment and redeployment phases, and the transition to and from war. *Commanders at all levels should participate in exercises to familiarize themselves with the complexities and details of IO doctrine and operations.* **Realistic exercises are essential for determining possible shortfalls and corrective actions to achieve success in future operations.** Various US non-DOD agencies, as well as foreign military services may occasionally participate in these training exercises. Commanders should continually assess the impact IO training, exercises, and ongoing peacetime missions have on their units' ability to conduct wartime missions.

At the very heart of warfare lies doctrine . . .

Suggested Reading

Arquilla, John and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Rand Corporation). 1997.

Baier, Frederick L., Capt, USAF, *50 Questions Every Airman Can Answer* (Air University Press). 1999.

Campen, Alan D., *The First Information War: The Story of Computers and Intelligence Systems in the Persian Gulf War* (AFCEA International Press). 1992.

Campen, Alan D., *Cyberwar: Security, Strategy, and Conflict in the Information Age* (AFCEA International Press). 1996

Daniel, Donald C., and Katherine L. Herbig and edited by John Gooch and Amos Perlmutter. "Propositions on Military Deception," *Military Deception and Strategic Surprise* (Frank Cass & Co.). 1982.

Denning, Dorothy, *Information Warfare and Security* (Addison Wesley Longman, Inc.). 1998.

Fitts, Richard E., Lt Col, USAF, ed. *The Strategy of Electromagnetic Conflict* (Peninsula Publishing). 1980.

Goldstein, Frank L., Col, USAF ed. *Psychological Operations: Principles and Case Studies* (Air University Press). 1996.

Keohane, O. and Joseph S. Nye, "Power and Interdependence in the Information Age" *Foreign Affairs.* Fall 1998.

Khalilzad, Zalmay and John White, *The Strategic Appraisal: The Changing Role of Information in Warfare,* (Rand Corporation). 1999.

Meilinger, Phillip S., Col USAF, *10 Propositions Regarding Air Power* (Air University Press). 1995.

Roszak, Theodore, *The Cult of Information: A Neo-Luddite Treatise on High-Tech, Artificial Intelligence, and the True Art of Thinking,* 2nd ed. (University of California Press). 1994.

Schleher, D. Curtis, Dr., *Introduction to Electronic Warfare* (Artech House). 1986.

Stein, George, Dr., and edited by G. Stocker and C. Schöpf, "Information Warfare: Words Matter" *InfoWar* (Springer). 1998.

Taylor, Philip M., *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day* (Manchester University Press). 1995.

Tsoukas, H., "The Tyranny of Light," *Futures*. November 1997.

Presidential Decision Directive. PDD-63, *Critical Infrastructure Protection.* 22 May 1998.

Presidential Decision Directive. PDD-68, *International Public Information.* 30 April 1999.

Joint Publications

Joint Publication 0-2, *United Action Armed Forces (UNAAF).*

Joint Publication 3-13, *Joint Doctrine for Information Operations.*

Joint Publication 3-53, *Doctrine for Joint Psychological Operations.*

Joint Publication 3-54, *Doctrine for Joint Operations Security.*

Joint Publication 3-56, *Doctrine for Joint Deception Operations.*

Air Force Doctrine Documents

Air Force Doctrine Document 2, *Organization and Employment of Aerospace Forces*. Accessible at http://www.doctrine.af.mil and http://afpubs.hq.af.mil

Air Force Doctrine Document 2-5.3, *Psychological Operations.* Accessible at http://www.doctrine.af.mil and http://afpubs.hq.af.mil

Air Force Doctrine Document 2-5.4, *Public Affairs Operations.* Accessible at http://www.doctrine.af.mil and http://afpubs.hq.af.mil

Military Publications

Air Force Pamphlet 51-45, *Electronic Combat Principles.*

Department of the Air Force. *Cornerstones of Information Warfare* (n.d.)(circa 1995).

Glossary

Abbreviations and Acronyms

ACO	airspace control order
ASETF	air and space expeditionary task force
AFCERT	Air Force Computer Emergency Response Team
AFDD	Air Force Doctrine Document
AFIWC	Air Force Information Warfare Center
AFNOC	Air Force Network Operations Center
AFOSI	Air Force Office of Special Investigations
AOC	air operations center
ATO	air tasking order
AWACS	Airborne Warning and Control System
C2	command and control
CERT	computer emergency response team
CI	counterintelligence
CINC	commander in chief
CISR	chief of intelligence, surveillance, and reconnaissance
CNA	computer network attack
CND	computer network defense
COA	course of action
COMAFFOR	commander, Air Force forces
COMSEC	communications security
DCA	defensive counterair
DCI	defensive counterinformation
DIW	defensive information warfare
DOD	Department of Defense
EA	electronic attack
EMSEC	emission security
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
GIG	Global Information Grid
GPS	global positioning system

I&W	indications and warning
IA	information assurance
IFDO	Informational Flexible Deterrent Options
IIW	information-in-warfare
IO	information operations
IP	Internet Protocol
IPB	intelligence preparation of the battlespace
IRM	information resource management
ISR	intelligence, surveillance, and reconnaissance
ISvs	information services
IT	information technology
IW	information warfare
IWF	information warfare flight
JCS	Joint Chiefs of Staff
JFASCC	joint force air and space component commander
JFC	joint force commander
JSCP	Joint Strategic Capabilities Plan
JSTARS	joint surveillance, target attack radar system
MAAP	Master Air Attack Plan
MAJCOM	major command
MOE	measures of effectiveness
NCA	National Command Authorities
NCC	Network Control Center
NOSC	Network Operations and Security Center
NOSC-D	Network Operations and Security Center (Deployable)
OCA	offensive counterair
OCI	offensive counterinformation
OIW	offensive information warfare
OODA	observe, orient, decide, and act
OPSEC	operations security
PA	public affairs
PNP	precision navigation and positioning
PSYOP	psychological operations
RSTA	reconnaissance, surveillance, target, and acquisition
STO	special technical operations

TMD	theater missile defense
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle

Definitions

air and space PSYOP. Deliberate use of air and space power, in any of its lethal or nonlethal, kinetic or nonkinetic, forms to achieve a psychological balance advantageous to friendly forces and objectives. PSYOP may be used offensively or defensively depending on the commander's intent and the current situation.

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called **C2.** (JP 1-02)

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA. Also called **CNA.** (JP 1-02)

computer network defense. Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Also called **CND.** (JP 1-02) The Air Force believes a more useful working definition for airmen is: *[CND is actions taken to plan and direct responses to unauthorized activity in defense of Air Force information systems and computer networks.]* {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

counterinformation. Counterinformation seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force. Counterinformation can be applied in an offensive (called **OCI**) or defensive (called **DCI**) manner.

cyberspace. The notional environment in which digitized information is communicated over computer networks. (JP 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (JP 1-02)

defensive counterinformation. Activities which are conducted to protect and defend friendly information and information systems. Also called **DCI.**

electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW.** The three major subdivisions within electronic warfare are:

a. electronic attack—That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called **EA.** EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

b. electronic protection—That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called **EP.**

c. electronic warfare support—That division of electronic warfare involving actions tasked by, or under direct control of, an operational

commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called **ES.** Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 1-02)

global information grid. 1. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data security services, and associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems. 2. Includes any system, equipment, software, or service that meets one or more of the following criteria:

a. transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services (see 3. below with respect to embedded information technology)

b. provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, or services

c. Processes data or information for use by other equipment software, and services.

3. The embedded information technology within a product is not considered part of the GIG; however, if it provides the functionality described in 2 above it must meet GIG interface criteria. Also called **GIG.**

information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 3-13.1) (JP 1-02)

information assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called **IA.** (JP 1-02)

information-in-warfare. IIW is a set of aerospace information operations functions that provides commanders battlespace situational awareness across the spectrum of conflict and range of air and space operations. IIW functions involve the Air Force's extensive capabilities to provide awareness throughout the range of military operations based on integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global navigation and positioning, weather, and communications capabilities. Also called **IIW.**

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO.** (JP 1-02) The Air Force believes that in practice a more useful working definition is: *[Those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare and information warfare.]* {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

information services. Air Force information services provide the infrastructure, communications pathways, computing power, applications support, information management, and network operations to make the GIG a reality. Elements of ISvs include: information assurance; applications; spectrum management; information resource management; establishment, operation, and sustainment of network; and information technology infrastructure. Also called **ISvs.**

information superiority. That degree of dominance in the information domain which permits the conduct of operations without effective opposition. Also called **IS.** (JP 2-01.3) (JP 1-02) The Air Force prefers to cast 'superiority' as a state of relative advantage, not a capability, and views **IS** as: *[That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.]* {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 3-13) (JP 1-02)

information warfare. Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called **IW.** (JP 1-02) The Air Force believes that, because the defensive component of IW is always engaged, a better definition is: *[Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems.]* {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

military deception. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02) [There are five categories of military deception. See JP 1-02 for complete definition.]

offensive counterinformation. Offensive IO/IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems. Also called **OCI.**

OODA Loop. A theory developed by Col John Boyd (USAF, Retired) contending that one can depict all rational human behavior, individual and organizational, as a continual cycling through four distinct tasks: observation, orientation, decision, and action.

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called **OPSEC.** (JP 1-02)

physical attack. When used in a counterinformation context, physical attack is the means to disrupt, damage, destroy, or alter adversary information or information systems through the conversion of stored energy into destructive power.

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called **PSYOP.** (JP 1-02)